getnet
www.getnet.com.tw

150Mbps Wireless IEEE802.11b/g/n 32-bit PCI Adapter

GN-531I

User Manual

Version 1.0 / January, 2010

Federal Communication Commission

Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

1. Reorient or relocate the receiving antenna.
2. Increase the separation between the equipment and receiver.
3. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
4. Consult the dealer or an experienced radio technician for help.

FCC Caution

This device and its antenna must not be co-located or operating in conjunction with any other antenna or transmitter.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Any changes or modifications not expressly approved by the party responsible for compliance could void the authority to operate equipment.

Federal Communication Commission (FCC) Radiation Exposure Statement

This equipment complies with FCC radiation exposure set forth for an uncontrolled environment. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 20cm (8 inches) during normal operation.

The antenna(s) used for this transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

The equipment version marketed in US is restricted to usage of the channels 1-11 only.

R&TTE Compliance Statement

This equipment complies with all the requirements of DIRECTIVE 1999/5/EC OF THE EUROPEAN PARLIAMENT AND THE COUNCIL of March 9, 1999 on radio equipment and telecommunication terminal Equipment and the mutual recognition of their conformity (R&TTE)
The R&TTE Directive repeals and replaces in the directive 98/13/EEC (Telecommunications Terminal Equipment and Satellite Earth Station Equipment) As of April 8, 2000.

Safety

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this and of the computer manufacture must therefore be allowed at all times to ensure the safe use of the equipment.

EU Countries Intended for Use

The ETSI version of this device is intended for home and office use in Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Luxembourg, the Netherlands, Portugal, Spain, Sweden, and the United Kingdom.

The ETSI version of this device is also authorized for use in EFTA member states: Iceland, Liechtenstein, Norway, and Switzerland.

EU Countries Not intended for use

None.

Copyright© by Edimax Technology Co, LTD. all rights reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual or otherwise, without the prior written permission of this company.

This company makes no representations or warranties, either expressed or implied, with respect to the contents hereof and specifically disclaims any warranties, merchantability or fitness for any particular purpose. Any software described in this manual is sold or licensed "as is". Should the programs prove defective following their purchase, the buyer (and not this company, its distributor, or its dealer) assumes the entire cost of all necessary servicing, repair, and any incidental or consequential damages resulting from any defect in the software. Further, this company reserves the right to revise this publication and to make changes from time to time in the contents hereof without obligation to notify any person of such revision or changes.

The product you have purchased and the setup screen may appear slightly different from those shown in this QIG. For more detailed information about this product, please refer to the User's Manual on the CD-ROM. The software and specifications are subject to change without notice. Please visit our web site www.getnet.com.tw. for the update. All right reserved including all brand and product names mentioned in this manual are trademarks and/or registered trademarks of their respective holders.

C A T A L O G

CHAPTER I: Product Information 1
1-1 Introduction and safety information 1
1-2 Safety Information 2
1-3 System Requirements 3
1-4 Package Contents 4
1-5 Familiar with your new wireless network card 5
CHAPTER II: Driver Installation and Configuration 6
2-1 Network Card Installation 6
2-2 Using the Wireless Configuration Utility 13
2-2-1 Using Ralink Utility 13
2-2-1-1 Scan for Other Wireless Devices 15
2-2-1-2 Connect to an Access Point 20
2-2-1-3 Add an Access Point to Profile 24
2-2-2 Using Windows Zero Configuration 32
2-3 Profile Management 36
2-3-1 Add a profile 37
2-3-2 Edit an existing profile 38
2-3-3 Delete an existing profile 39
2-3-4 Activate a profile 40
2-4 Advanced Settings 41
2-5 View Network Statistics 44
2-6 WMM Setting 45
2-7 WPS Configuration 47
2-7-1 WPS Setup - PBC (Push-Button Configuration) 48
2-7-2 WPS Setup - PIN 51
2-8 Radio On/Off 53
2-9 About 54
2-10 On-line Help 55
CHAPTER III: Soft-AP Function 56
3-1 Switch to AP Mode and Basic Configuration 56
3-2 Security Setting 61
3-3 Access Control 64
3-4 Connection Table 66
3-5 Event Log 68
3-6 Statistics 69
3-7 About 70

CHAPTER IV: Appendix 71
4-1 Specification 71
4-2 Troubleshooting 72
4-3 Glossary 74

CHAPTER I: Product Information

1-1 Introduction and safety information

Thank you for purchasing this high-speed wireless network card! Excepting common wireless standards 802.11b/g, this wireless network card is also able to access 802.11n wireless networks - data transfer rate is 150Mbps, and that's three times faster than 802.11g wireless network!

With easy-to-install PCI interface - a very common expansion port of computers - plug this wireless network card into any empty PCI slot of your computer, just that simple!

Other features of this wireless network card including:

- High-efficiency antenna expands the scope of your wireless network.
- High-speed data transfer rate - Up to 150Mbps.
- WMM function: control the bandwidth required for different applications.
- Work with IEEE 802.11b/g/n wireless devices.
- Supports major encryption methods like WEP, WPA, and WPA2 encryption.
- WPS configuration - You don't need an experienced computer technician to help you to get connected. Utilizing the software program of the card, you can get your computer connected by pushing a button or entering an 8-digit code. Pressing the button on the network card, the WPS connection can be activated as well.
- PCI interface - you can get it installed on your computer in just few seconds!

1-2 Safety Information

In order to keep the safety of users and your properties, please follow the following safety instructions:

1. This wireless network card is designed for indoor use only. DO NOT expose this network card to direct sun light, rain, or snow.

2. DO NOT put this network card at or near hot or humid places, like kitchen or bathroom. Also, do not left this wireless network card in the car in summer.

3. This network card will become hot when being used for long time (***This is normal and is not a malfunction)***. DO NOT put the network card on a paper, cloth, or other flammable objects after the network card has been used for a long time.

4. There's no user-serviceable part inside the network card. If you found that the network card is not working properly, please contact your dealer of purchase and ask for help. DO NOT disassemble the network card by your self, warranty will be void.

5. If the network card falls into water, DO NOT USE IT AGAIN BEFORE YOU SEND THE CARD TO THE DEALER OF PURCHASE FOR INSPECTION.

6. If you smell something strange or even see some smoke coming out from the network card, switch the computer off immediately, and call dealer of purchase for help.

1-3 System Requirements

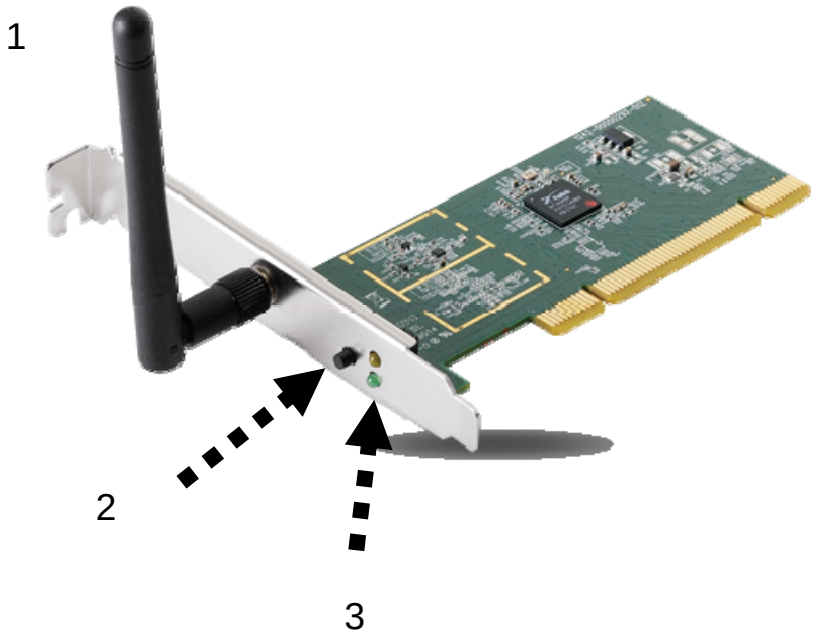
- An empty PCI slot
- Windows 2000, XP, Vista, or Windows 7 operating system
- CD-ROM drive
- At least 100MB of available disk space

1-4 Package Contents

Before you starting to use this wireless network card, please check if there's anything missing in the package, and contact your dealer of purchase to claim for missing items:

- ☐ PCI Wireless Network Card (1 pcs) ……. 1
- ☐ 2dBi Dipole Antenna (1 pcs) ……..……. 2
- ☐ Quick Installation Guide (1 pcs) ……..……. 3
- ☐ Driver/Utility/User Manual CD-ROM (1pcs) …..…… 4

1-5 Familiar with your new wireless network card



1. Antennas

One 2dBi dipole antenna is enclosed with the PCI card. Please secure the antenna to Reverse SMA connector of the card.

2. WPS Button

Press this button and hold for 3 seconds to start WPS function. When WPS is enabled, the Link and Tx/Rx LEDs will be steadily on.

3. Link and Tx/Rx LED Definitions

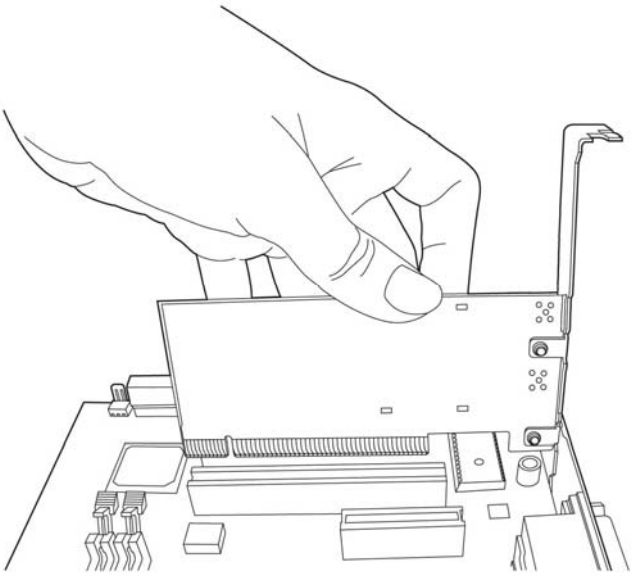
LED Name	Light Status	Description
Link	On	Link to a wireless access point
	Off	Radio is switched to off.
Tx/Rx	Blinking	Transferring / receiving data
	Off	No wireless activity

CHAPTER II: Driver Installation and Configuration

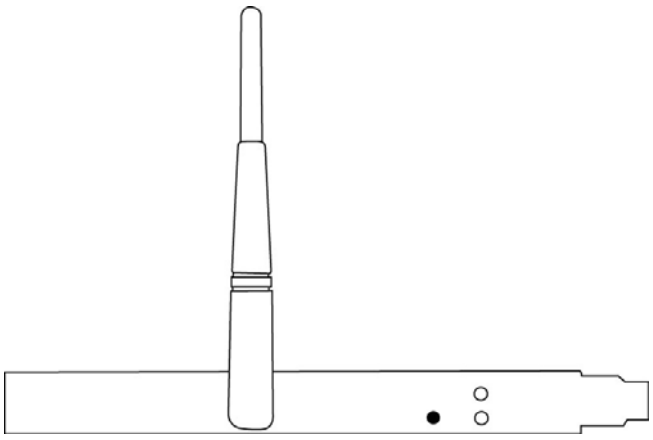
2-1 Network Card Installation

Please follow the following instructions to install your new wireless network card:

1. SWITCH THE COMPUTER OFF, remove the cover and insert the wireless network card into an empty PCI slot of your computer and then replace the cover.



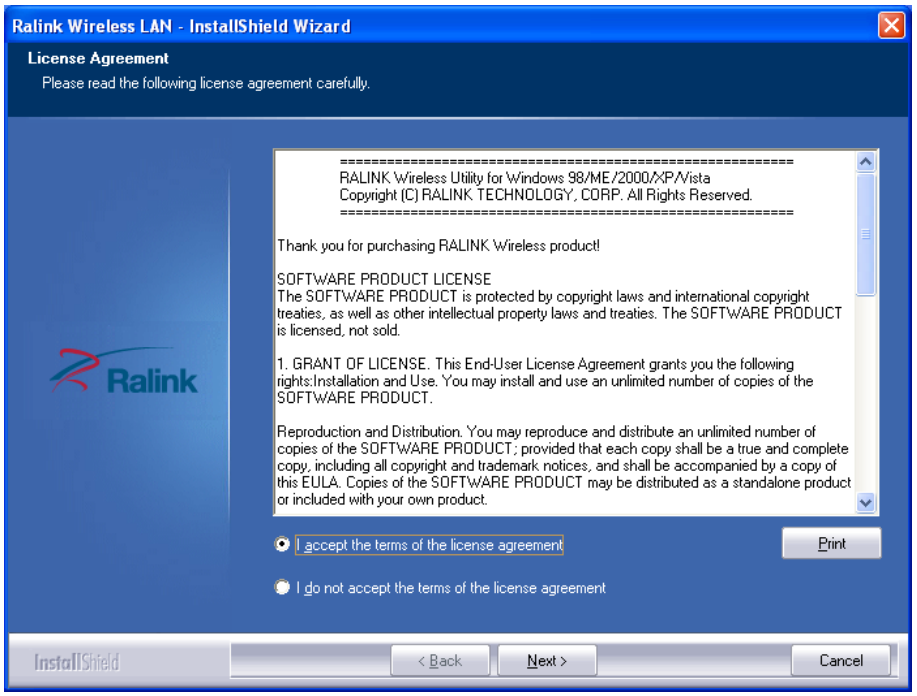
2. Install the antenna on the wireless network card, and make sure the antenna is securely installed. To improve radio reception, please adjust antenna to the proper position.



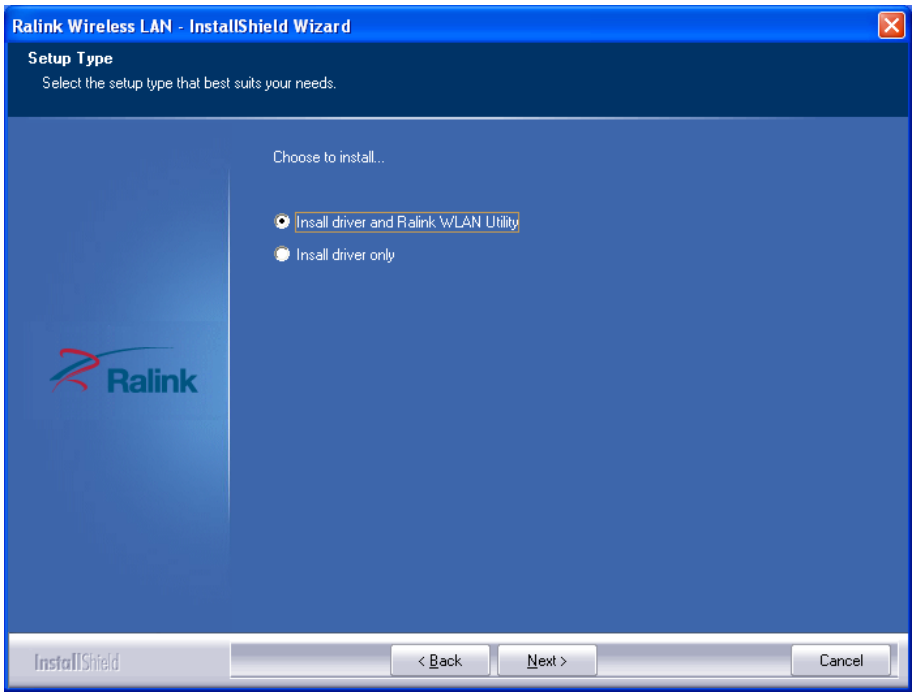
3. When you restart the computer, this ‘Found New Hardware Wizard’ screen will appear, click ‘Cancel’.

Found New Hardware Wizard
Welcome to the Found New Hardware Wizard
Windows will search for current and updated software by looking on your computer, on the hardware installation CD, or on the Windows Update Web site (with your permission).
Read our privacy policy
Can Windows connect to Windows Update to search for software?
Yes, this time only
Yes, now and every time I connect a device
No, not this time
Click Next to continue.
< Back
Next >
Cancel

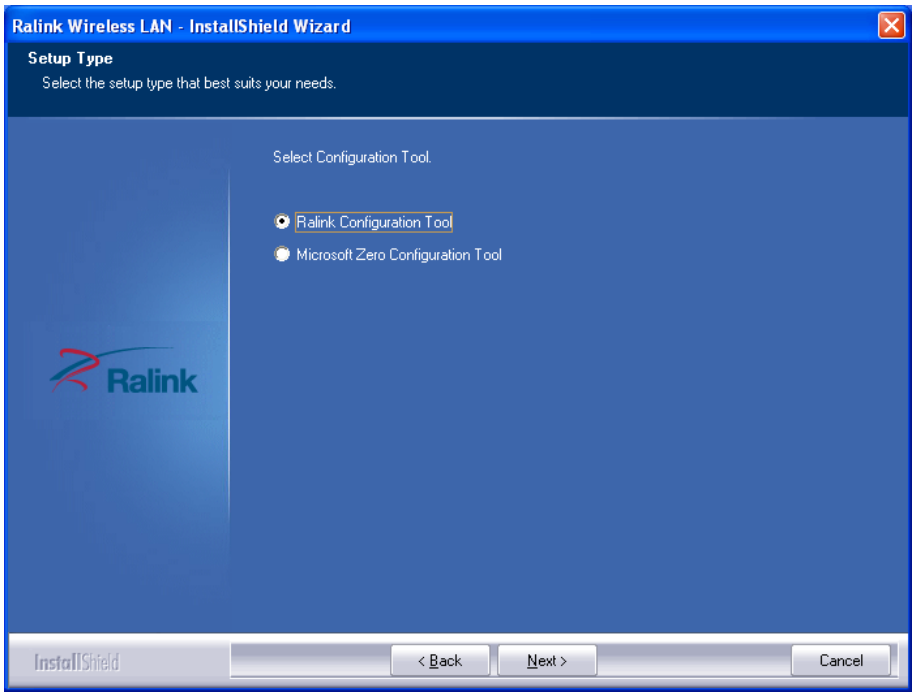
4. Insert device driver CDROM into the CD/DVD ROM drive of your computer, and execute ‘Setup.exe’ program. Please read the end user license agreement and click ‘I accept the terms of the license agreement’ then click ‘Next’ button, to accept license agreement.


Ralink Wireless LAN - InstallShield Wizard
License Agreement
Please read the following license agreement carefully.
RALINK Wireless Utility for Windows 98/ME/2000/XP/Vista
Copyright (C) RALINK TECHNOLOGY, CORP. All Rights Reserved.
Thank you for purchasing RALINK Wireless product!
SOFTWARE PRODUCT LICENSE
The SOFTWARE PRODUCT is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. The SOFTWARE PRODUCT is licensed, not sold.
1. GRANT OF LICENSE. This End-User License Agreement grants you the following rights:Installation and Use. You may install and use an unlimited number of copies of the SOFTWARE PRODUCT.
Reproduction and Distribution. You may reproduce and distribute an unlimited number of copies of the SOFTWARE PRODUCT; provided that each copy shall be a true and complete copy, including all copyright and trademark notices, and shall be accompanied by a copy of this EULA. Copies of the SOFTWARE PRODUCT may be distributed as a standalone product or included with your own product.
I accept the terms of the license agreement
I do not accept the terms of the license agreement
Print
Ralink
InstallShield
< Back
Next >
Cancel

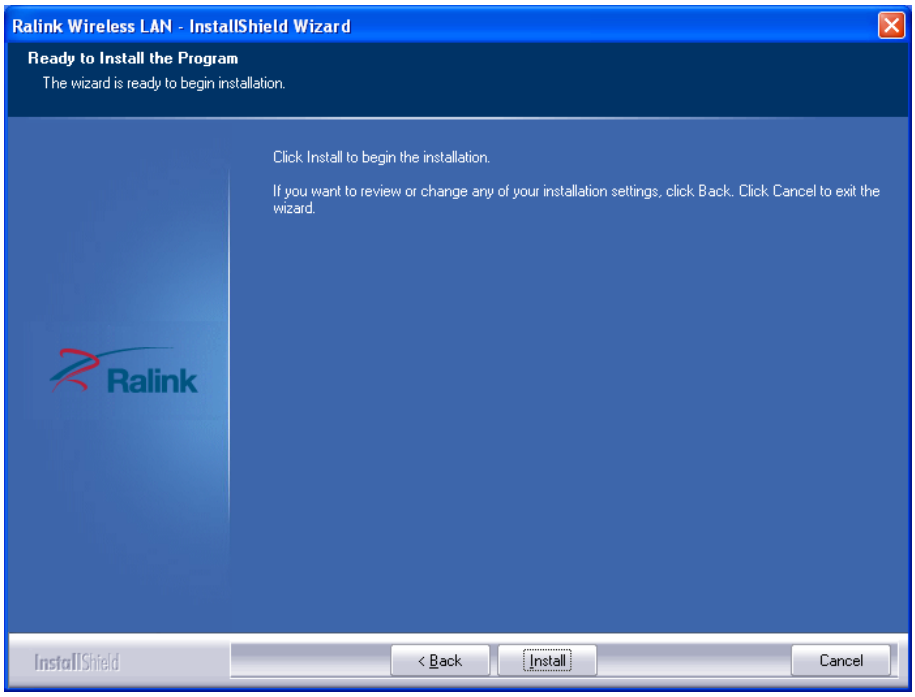
5. It is recommend installing driver and utility if the network card is installing the first time. If you want to update the driver only, choose ’Install driver only’. Click ‘Next’ to continue.



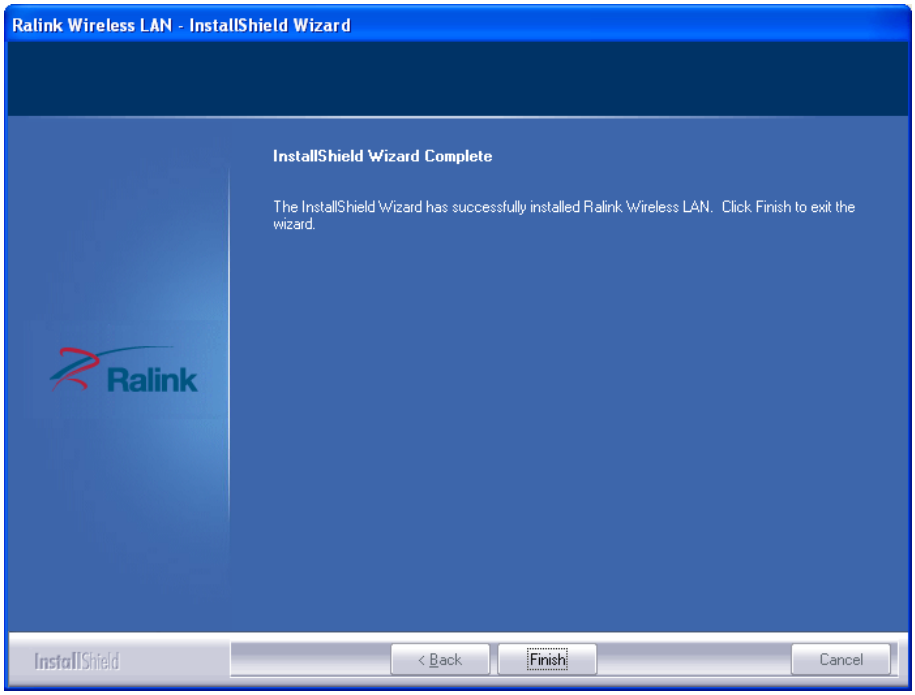
6. You can choose the configuration tool used to configure the wireless network card here. It’s recommended to select ‘Ralink Configuration Tool’, which provides fully access to all functions of this wireless network card. If you prefer to use the wireless configuration tool provided by Windows XP, please select ‘Microsoft Zero Configuration Tool’ then click ‘Next’.



7. Now you'll see the following message, please click 'Install' to start utility installation. **If you see 'Found New Hardware' message again, please ignore it and wait.**


Ralink Wireless LAN - InstallShield Wizard
Ready to Install the Program
The wizard is ready to begin installation.
Click Install to begin the installation.
If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.
Ralink
InstallShield
< Back
Install
Cancel

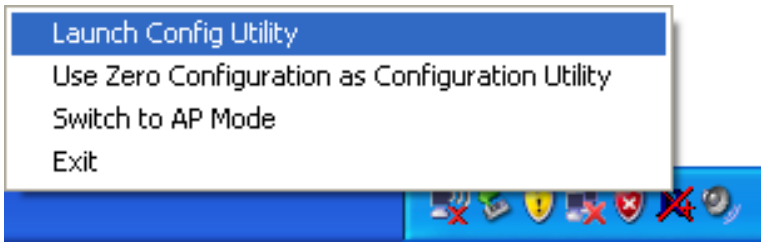
8. Please wait while the install procedure is running. When you see this message, please click ‘Finish’ to complete the driver installation process.



9. After installation is complete, wireless configuration utility will be shown in the desktop of your computer automatically. You will also see an icon at the lower-right corner of your windows system. If you put the mouse cursor on the icon, the status of wireless card will be displayed as a popup balloon.

When you want to configure your wireless connection, please right click on this icon, and a popup menu will appear. You can click 'Launch Config Utility' to start configuration program.

If you want to close the configuration utility, please click 'Exit'.



Please note that if you stopped config utility by 'Exit' function, you'll not be able to maintain the wireless link to the access point you wish to use. In this case, you can start config utility again by clicking 'Ralink Wireless Utility' icon from 'Start' -> 'All Programs' -> 'Ralink Wireless', as shown below.

fae
Internet
Internet Explorer
E-mail
Outlook Express
MSN
Windows Media Playe
Windows Messenger
Tour Windows XP
Files and Settings Tra
Wizard
Paint
All Programs
My Documents
My Recent Documents
Set Program Access and Defaults
Windows Catalog
Windows Update
Accessories
Games
Ralink Wireless
Startup
Internet Explorer
MSN
Outlook Express
Remote Assistance
Windows Media Player
Windows Messenger
Windows Movie Maker
Ralink Wireless Utility
Uninstall - RT2870
Log Off
Turn Off Computer
start

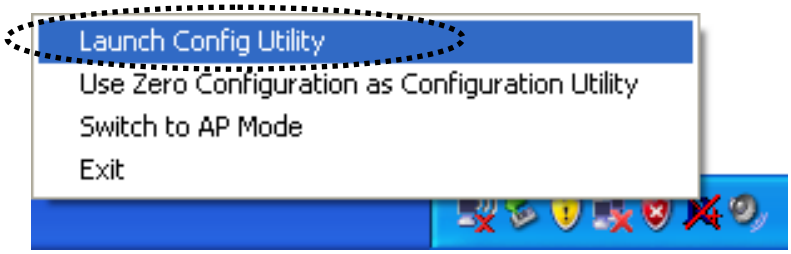
2-2 Using the Wireless Configuration Utility

There are two ways you can configure your wireless network card to connect to wireless access point: using the Ralink configuration utility and using built-in windows zero configuration utility.

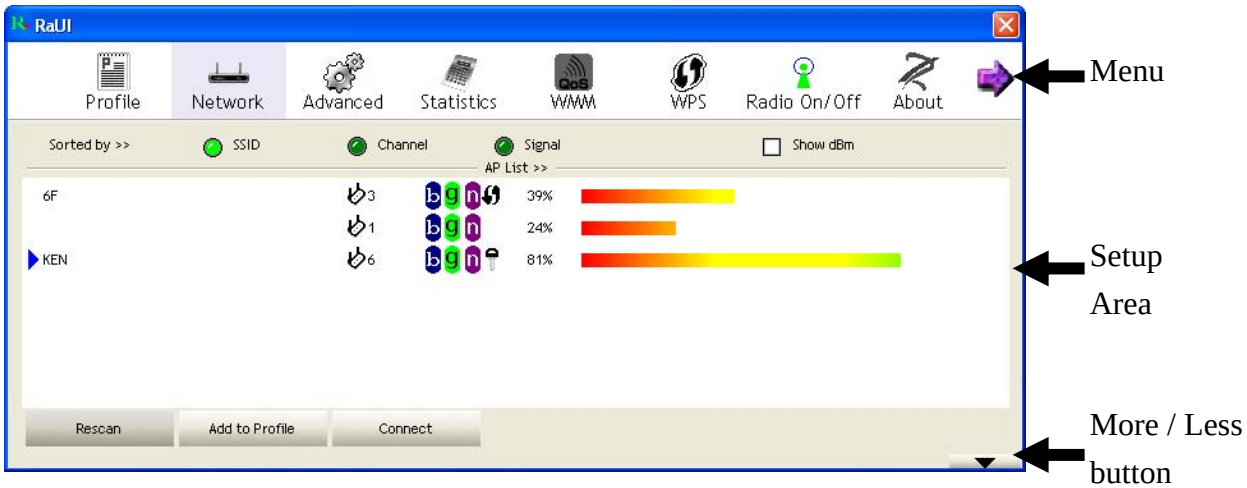
2-2-1 Using Ralink Utility

Please follow the following instructions to use Ralink configuration utility to connect to wireless access point.

1. Right-click the Ralink configuration utility icon located at lower-right corner of computer desktop and then clicks ‘Launch Config Utility’.

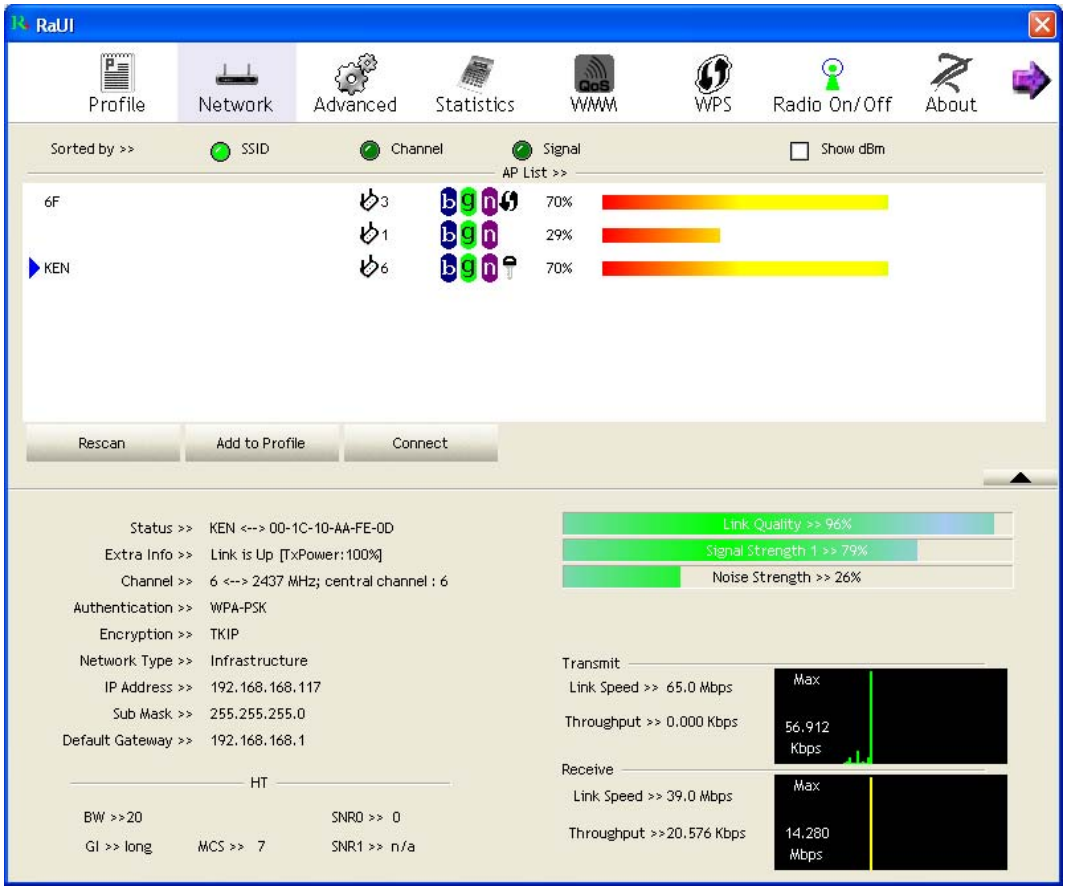


2. Ralink setup utility (RaUI) will launch, and begin to scan for all wireless access points automatically.



RaUI consists two parts: Menu and setup area. You can select a setup function (Profile, Network, etc.) from menu, and corresponding setup items will be displayed at setup area.

Some function includes more information, and can not be fitted in setup area. In this case, you can click ‘More / less’ button to expand the setup utility window, to display more information:



You can click ‘More / Less’ button again, and setup utility window will resume to its original size.

Tip: If a setup item requires more information to complete the setup procedure, the setup utility window will expand automatically.

2-2-1-1 Scan for Other Wireless Devices

There are two kinds of wireless connection mode: Infrastructure and Ad-Hoc. Infrastructure mode is used by wireless access points, which is able to establish wireless connection for you and other wireless / wired network clients.

Ad-Hoc mode is also know as ‘point-to-point’ mode, and in this mode, wireless devices such as computer or PDA will not be capable to establish wireless connection with more than one wireless device, and is suitable for establishing a one-to-one wireless connection between two wireless devices.

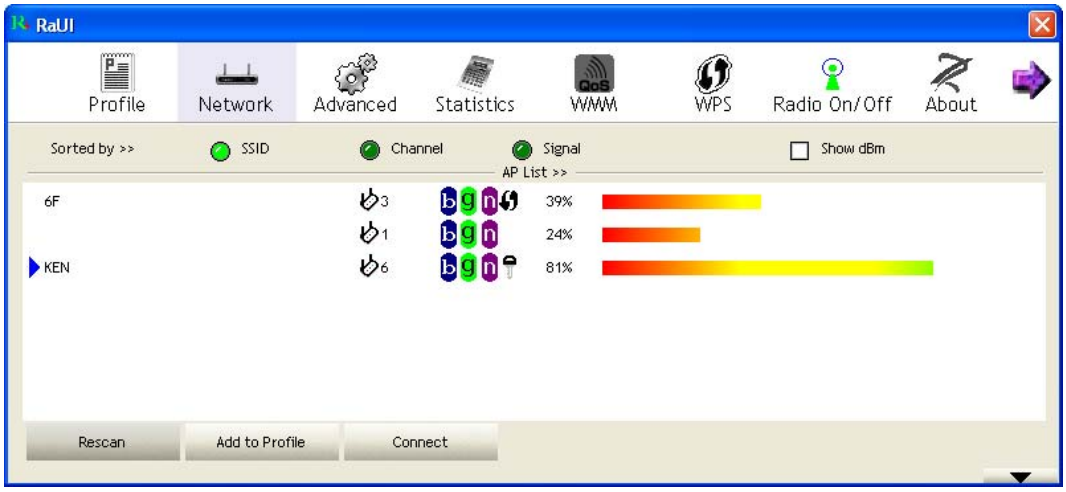
Before you can connect to any wireless access point or device by infrastructure or Ad-Hoc mode, there two things you must know:

a. Wireless device’s ‘SSID’ (Service Set IDentifier, someone will call it ‘access point’s name’).

   You can scan for the SSID of other wireless devices nearby, but if the SSID of the wireless device you wish to connect is hidden, you must know exact SSID before you can establish connection with it.

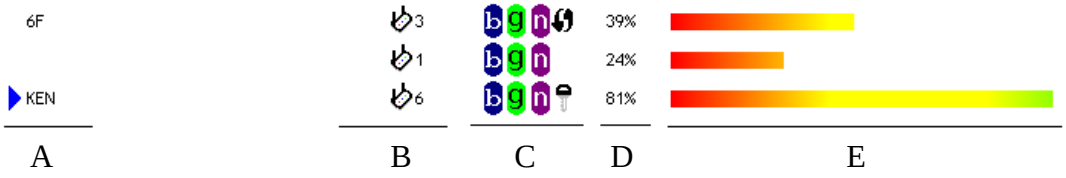
b. If the wireless device you wish to connect uses encryption, you must know its encryption key.

Please launch Ralink setup utility and it will scan for wireless access points near by:



Scan results will be displayed here, please check if the wireless device (access point or another computer) with the SSID you wish to connect is shown here.

Scan result includes 6 types of information, they are:



A The SSID (Service Set Identifier) of wireless device. If nothing is displayed here, it means the SSID of this wireless device is hidden.

If a ▶ symbol appears in front of the name of wireless device, means you've established connected with that wireless device.

B The type of this wireless device and the channel number of this wireless device.

Means this wireless device is an access point

Means this wireless device is a computer (Ad-Hoc mode, point-to-point connection)

C The wireless standard supported by this access point is displayed here.

'n' for 802.11n *, 'g; for 802.11g* *, and 'b' for 802.11b* *. WPS icon* *will appear when the access point supports WPS. If the access point uses encryption, a key icon* *will appear.*

Note: When the access point supports WPS and WPS icon *is appeared, you will not see the key icon* *here even through the access point uses encryption.*

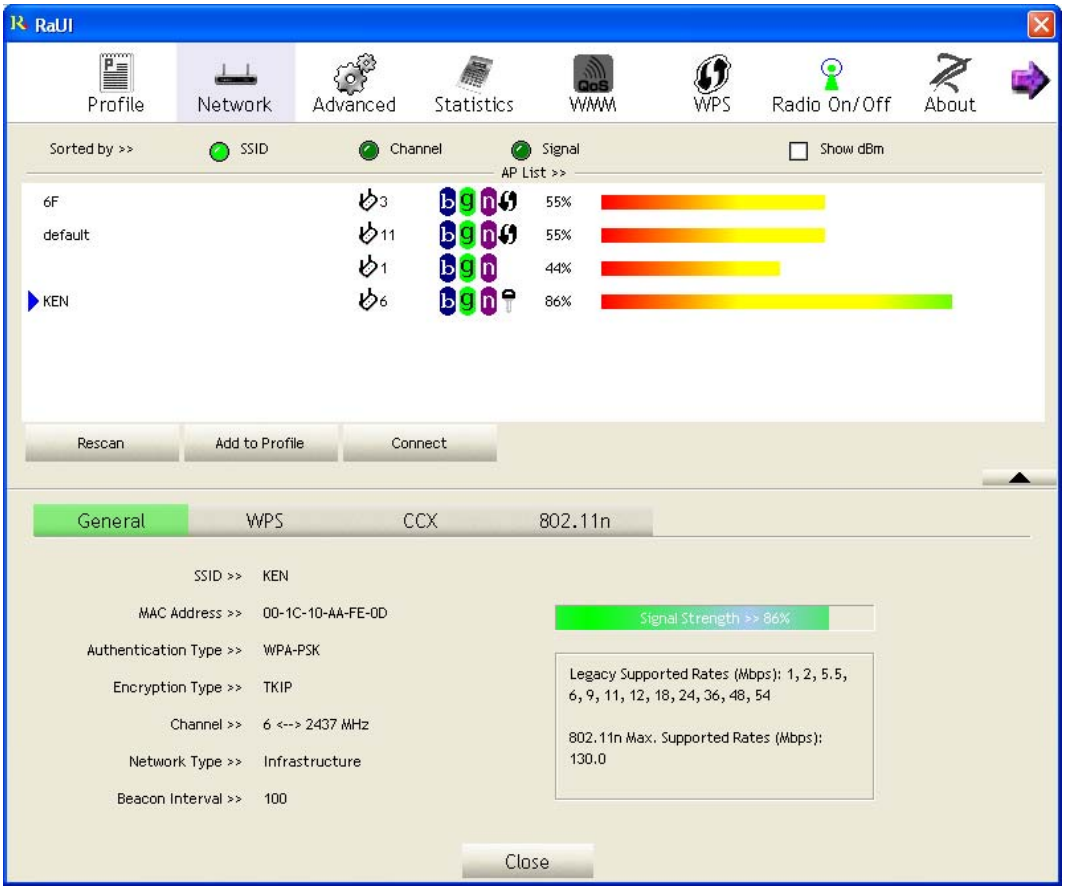
D Shows the signal strength of access point by percentage.

E Shows the bar graph of the signal strength.

If you can not see the access point you wish to connect here, please click 'Rescan' button to scan for access point again, until the one you preferred is displayed. You may have to click 'Rescan' for more than two times before you can see the access point you wish to use here.

If you still can not see the access point you wish to use after clicking 'Rescan' for more than five times, please move your computer closer to the location where the wireless access point is, or see instructions in Chapter 4-2 'Troubleshooting'.

If you wish to see detailed information for a specific access point, please double-click on it, and you'll be provided with its detailed information.



There are 4 types of technical information:

General: Displays basic information about this access point, such as SSID, MAC Address, authentication / encryption type, channel etc.

WPS: If this access point supports WPS (Wi-Fi Protected Setup), related information will be displayed here.

CCX: If this access point supports CCX (Cisco Compatible eXtension), related information will be displayed here.

802.11n: If this access point complies with 802.11n draft, related information will be displayed here.

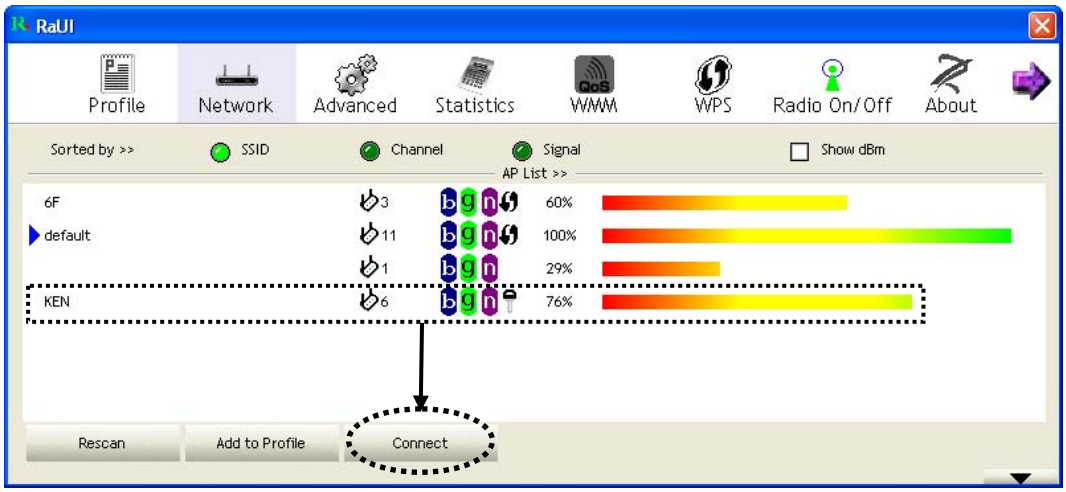
And here are descriptions of every setup item in setup area:

Item Name	*Description*
Sorted by >>	You can decide how to sort all listed access point by ‘SSID’, ‘Channel’, or ‘Signal’ (signal strength).
Show dBm	Check this box to show the signal strength of access point, instead of percentage.
Rescan	Click this button to rescan access points. You can click this button for several times, if the access point you wish to use does not show in the list.
Add to Profile	You can store a specific access point to profile, so you can link to that access point directly next time, without inputting authentication key again. To add an access point to profile, you have to select an access point from the list first, then click ‘Add to Profile’ button. Detailed instructions will be given below.
Connect	Connect to a selected access point. You have to select an access point from the list first and then click ‘Connect’ to connect to the selected access point.

2-2-1-2 Connect to an Access Point

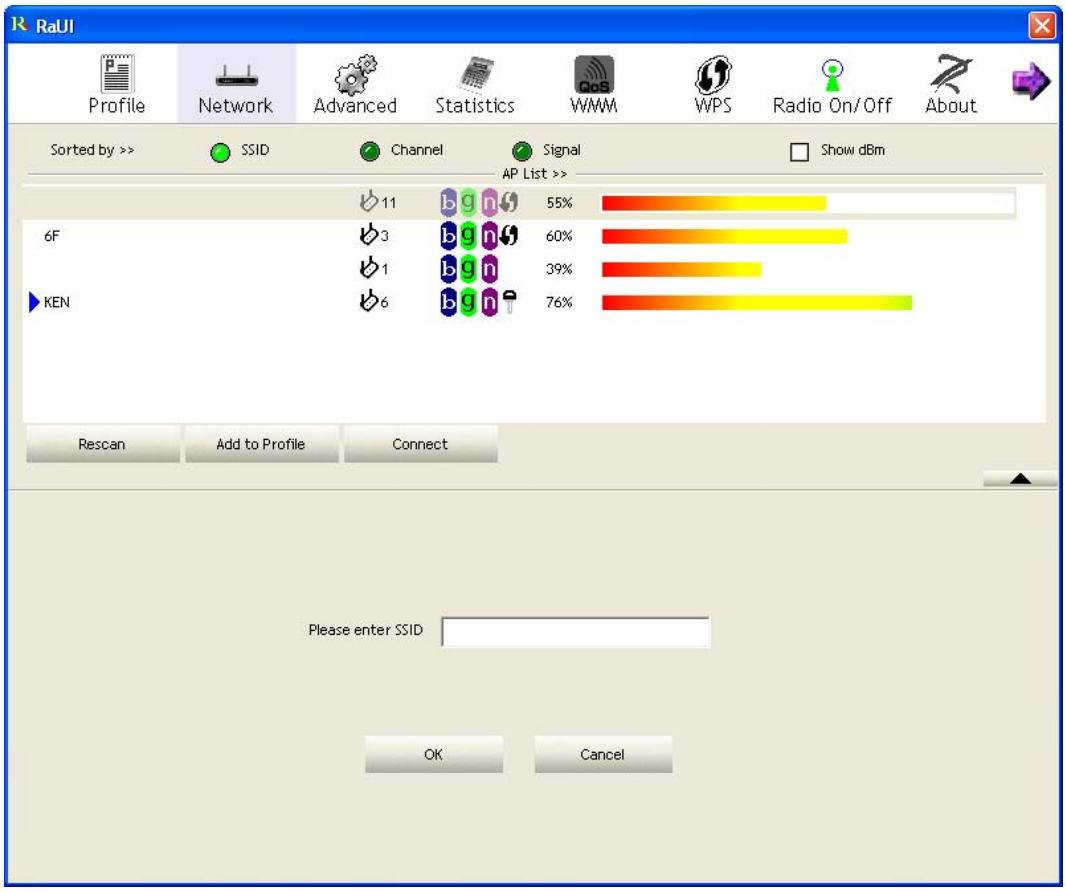
If the wireless access point you wish to connect is found, you can establish connection with it by clicking ‘Connect’ button. Instructions will be given as follow:

1. Click the wireless access point or network device you wish to connect, it will be highlighted, then click ‘Connect’.

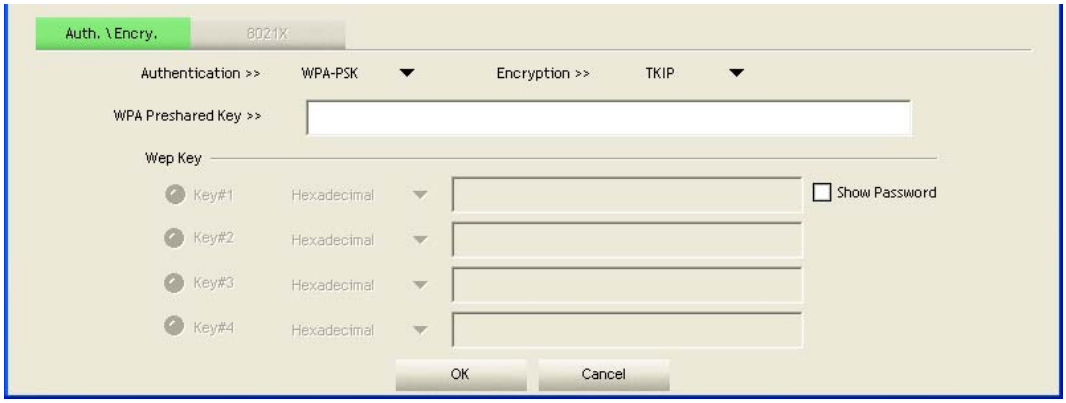


   If the access point you selected does not use encryption, you’ll be connected to this wireless access point within one minute. If the access point you selected uses encryption, please proceed to step 3.

2. If the wireless access point does not have SSID, you’ll be prompted to input it now. Please ask the owner of wireless access point for the exact SSID and input it here, then click ‘OK’ when ready. If the SSID you provided here is wrong, you’ll not be able to connect to this access point.



3. If the wireless access point uses encryption, you will be prompted to input its WEP key or WPA preshared key.



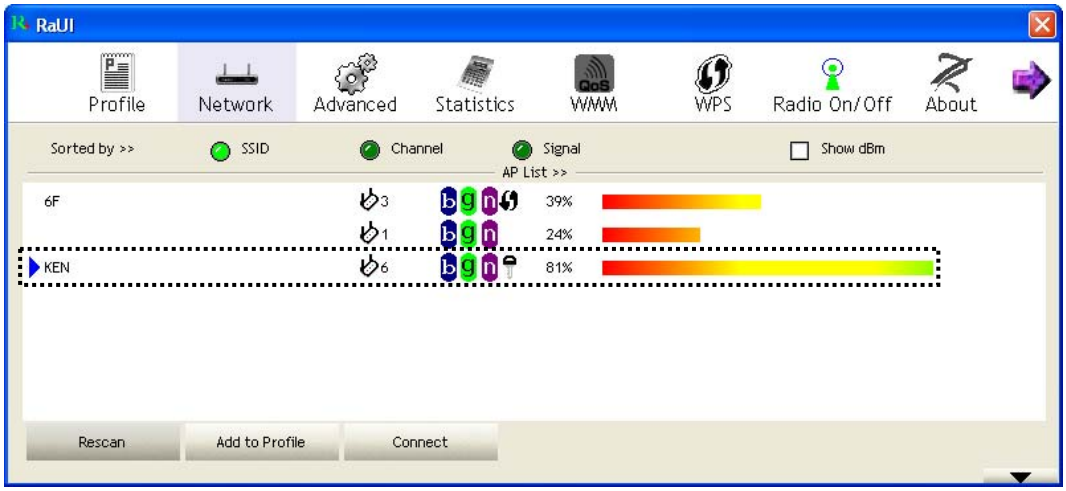
4. Please ask the owner of the wireless access point you want to connect, and input the correct key here and then click ‘OK’. By checking ‘Show Password’ box, the encryption key you inputted here will be displayed.

   If the value you inputted here is wrong, you will not be able to connect to this wireless access point.

   Authentication type will be selected by the authentication type of the access point automatically, please don’t change it.

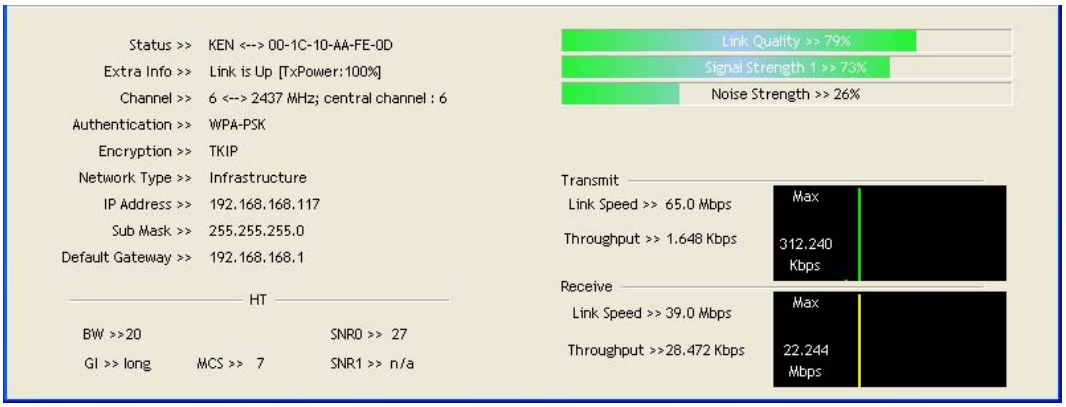
   However, if you’re connecting to an access point uses 802.1x authentication, you have to check ‘802.1x’ box and input related information. Instructions for 802.1x authentication will be given later.

5. If the wireless access point is successfully connected, you’ll see a ▶ symbol appears in front of the name of wireless device.



You can put the mouse cursor over the Ralink configuration utility icon, and the brief information about link status and signal strength of current wireless connection will be shown as a popup balloon.

You can also click More / Less button ( ) to see detailed information of connected access point:



The current status of wireless connection will be displayed by Ralink configuration utility icon:

Wireless connection is established, good signal reception.

Wireless connection is established, normal signal reception.

Wireless connection is established, weak signal reception.

Connection is not established yet.

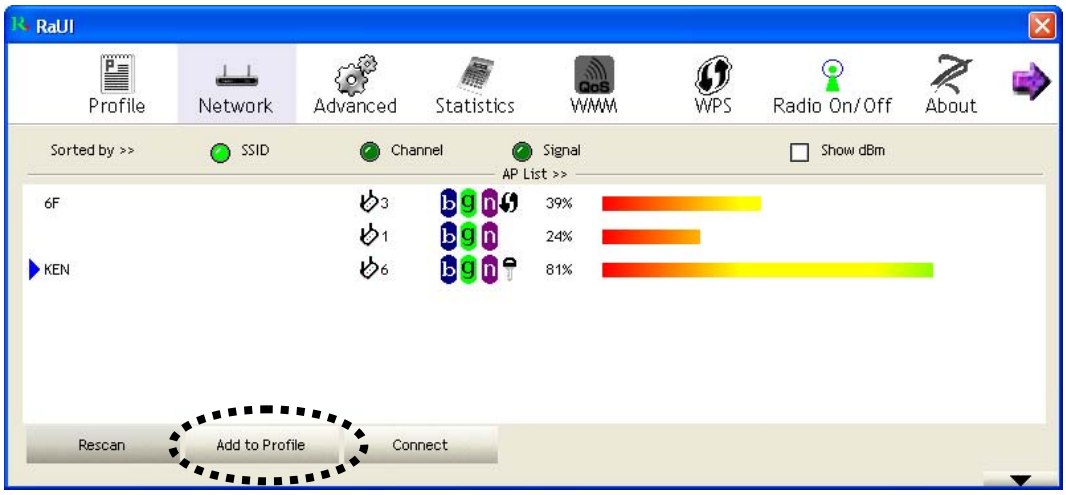
Wireless network card is not detected.

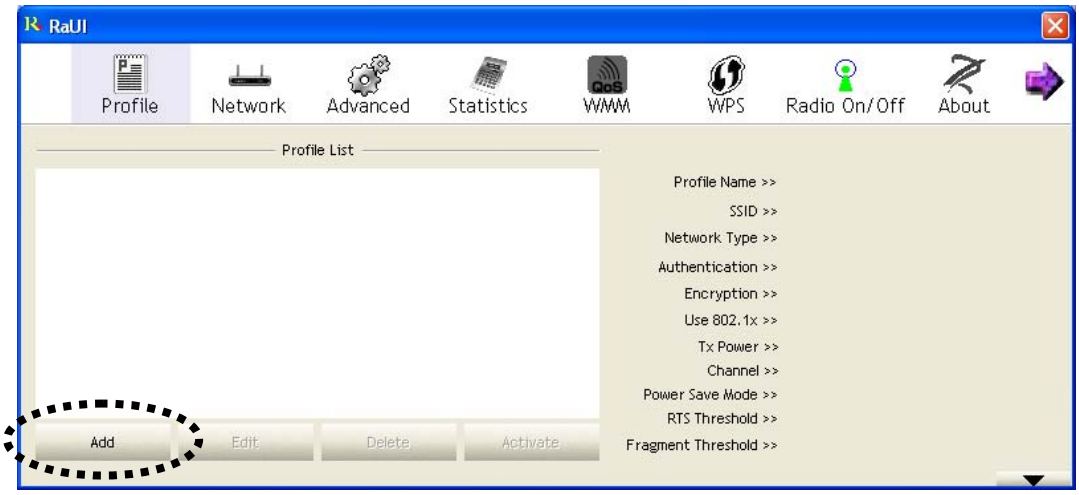
2-2-1-3 Add an Access Point to Profile

If you will connect to some specific wireless access point frequently, you can add their information to the profile. Just like the telephone directory, the profile saves all information of access points, and you can recall them anytime you wish to establish connection.

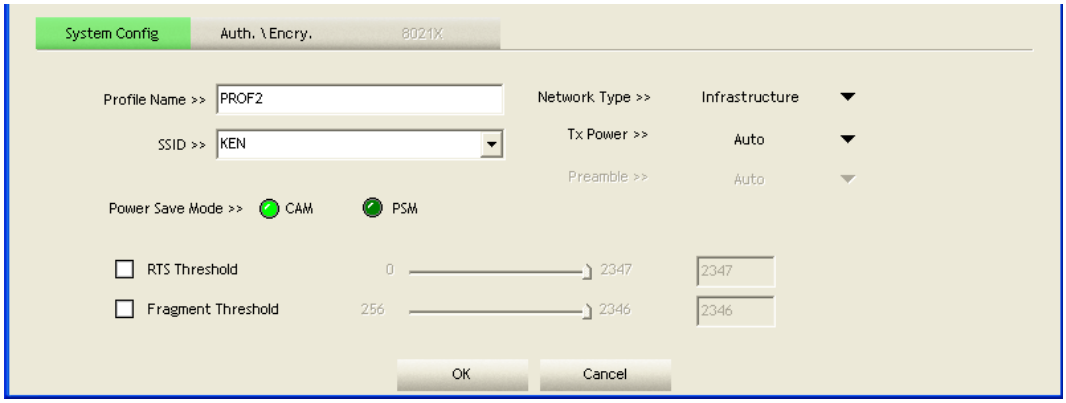
You can add a found access point to profile, or input all information of an access point by yourself.

To add a found access point to profile, please select a found access point first (to make it highlighted), then click ‘Add to Profile’ button; to input the information of access point by yourself, please go to ‘Profile’ menu and click ‘Add’ button.





The setup utility will expand:

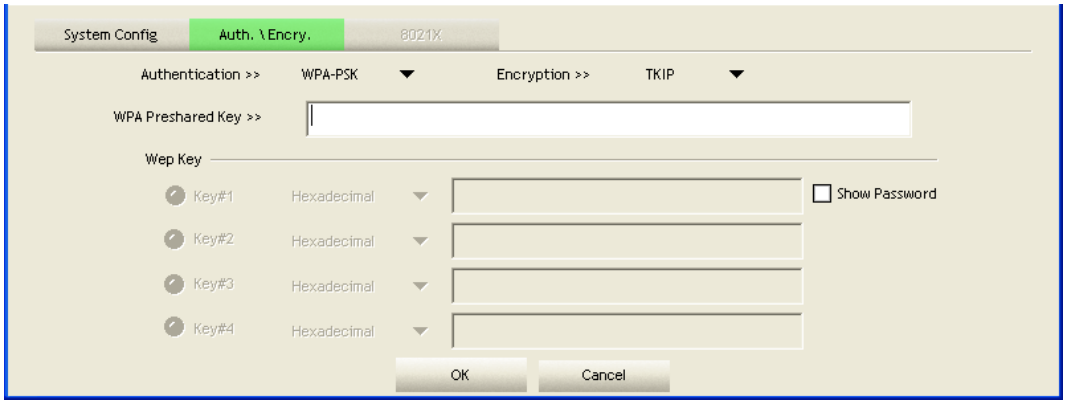


Here are descriptions of every setup item:

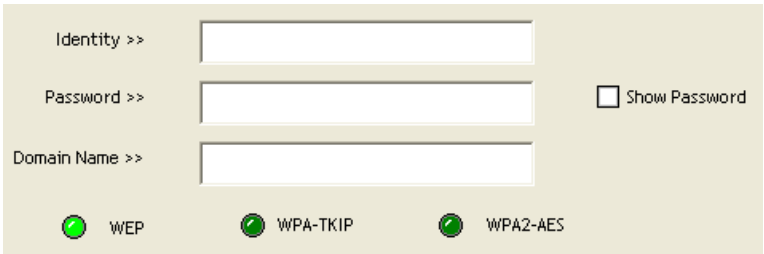
Item Name	*Description*
Profile Name	You can give this profile a name. Every profile needs a unique name.
SSID	Please input the SSID of this access point. If you selected an access point from the list, and its SSID is not hidden, the SSID will be filled automatically; however, you can modify the SSID by yourself.
Network Type	Please select the network type: Ad hoc or Infrastructure. If you're connecting to an access point, please select 'Infrastructure'; for point-to-point wireless connection (i.e. connecting to another computer using Ad Hoc mode), please select Ad hoc here. If you selected an access point from the list above, please keep this field unchanged.
Tx Power	You can select the wireless output power here. If you're not too far from access point (good signal reception), you can select a lower output power to save energy; for a distant access point, you can select a higher output power. It's suggested to select 'Auto' to let setup utility

	decide the best output power for you.
Preamble	Select the preamble for Ad hoc mode here. Available options are ‘Auto’ and ‘Long’. It’s suggested to select ‘Auto’ to let setup utility decide the preamble for you.
Channel	You can select the radio channel number for AdHoc mode here.
Power Save Mode	Please select CAM (constantly awake mode, keep wireless radio activity even when not transferring data), or PSM (Power saving mode, switches radio off when not transferring data). It’s recommended to choose ‘PSM’ if you’re using this network card with notebook computer to help the battery live longer.
RTS Threshold	Check this box to set the RTS threshold by yourself. You can drag the slider to set the threshold value, or input the value in the box located at right. It’s recommended to keep this value untouched unless you know the effect of changing this value.
Fragment Threshold	Check this box to set the packet fragment threshold by yourself. You can drag the slider to set the threshold value, or input the value in the box located at right. It’s recommended to keep this value untouched unless you know the effect of changing this value.

To set authentication / encryption information for the access point. Please click ‘Auth. \ Encry.’ tab:

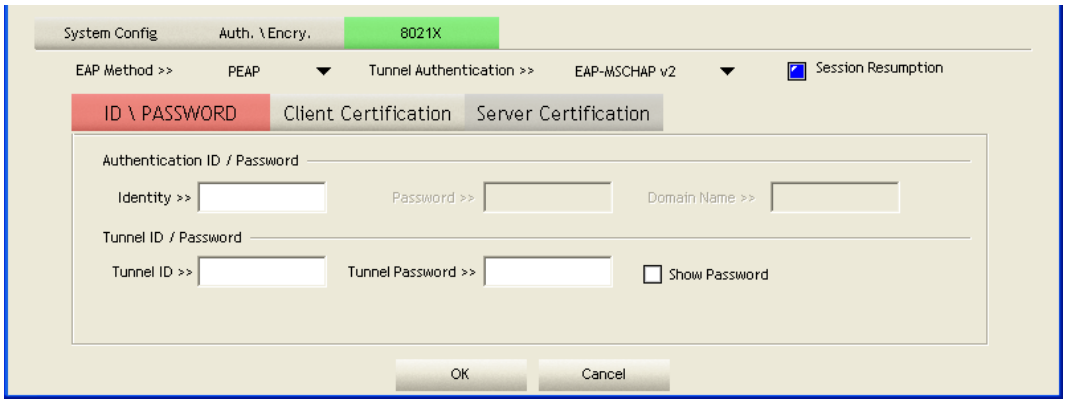


Here are descriptions of every setup item:

Item Name	*Description*
Authentication	Select the authentication type of the wireless access point or wireless device you wish to connect. When you’re adding a profile from an existing access point or wireless device, authentication type will be selected automatically, and please do not change it. If you select ‘LEAP’, you’ll be prompted to input LEAD specific settings:  Please input LEAP identity, password, domain name, and select encryption type. You can check ‘Show Password’ box so the password you inputted will be displayed as you type, but not replace by asterisk.
Encryption	Select the encryption type of the wireless access point or wireless device you wish to connect. When you’re adding a

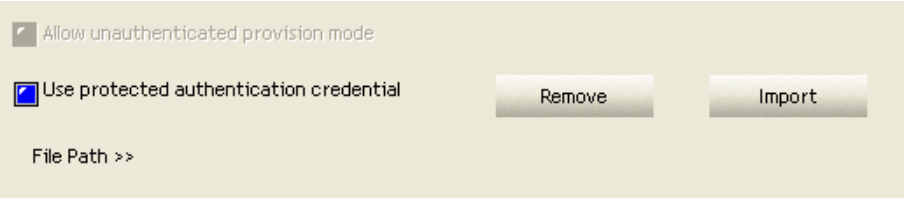
	profile from an existing access point or wireless device, the encryption type will be selected automatically, and please do not modify it.
WPA Preshared Key	Input WPA preshared key here. If encryption is not enabled, or you select ‘WEP’ as encryption type, this field will be disabled and grayed out.
WEP Key	You can select key type (Hexadecimal or ASCII) and input WEP key here. If encryption is not enabled, or you select ‘WPA’ as encryption type, this field will be disabled and grayed out. You can set up to 4 WEP keys here. There are two types of WEP key: Hexadecimal and ASCII. For Hexadecimal key, you can input number 0-9 and alphabet a-f; for example, ‘001122aabbcc’; For ASCII key, you can input number 0-9 and alphabet a-z; for example, mywepkey12345. The length of WEP key depends on the type of WEP key you selected. You can input 10 or 26 hexadecimal characters and 5 or 13 ASCII characters as WEP key.
Show Password	Check this box and all passphrases or security keys you inputted will be displayed as you type, but not replace your input with asterisk.
Use 802.1x	If the access point you wish to connect requires 802.1x authentication, please click on ‘Use 802.1x’ box, then click ‘802.1X’ tab to set 802.1x parameters.

To set 802.1x authentication for the access point. Please click ‘802.1X’ tab:



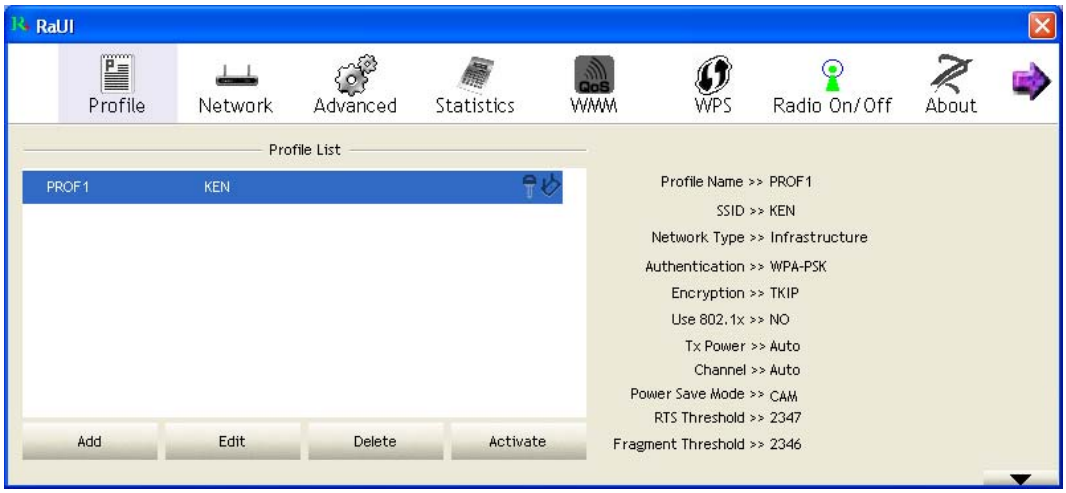
Here are descriptions of every setup item:

Item Name	*Description*
EAP Method	Select 802.1x EAP method from dropdown menu. Please ask the administrator of the access point you wish to connect to select a correct EAP method.
Tunnel Authentication	Select 802.1x tunnel authentication type from dropdown menu. Please ask the administrator of the access point you wish to connect to select a correct tunnel authentication method. This pull down menu is only available when authentication type you use is 'PEAP', ‘TLS / Smart Card', or 'TTLS'. When you use 'EAP-FAST' as authentication type, the protocol setting is always 'Generic Token Card' and can not be changed. You also need to select ‘Soft Token’ or ‘Static Password’ as password in ‘ID \ Password’ setting. ’EAP Fast’ authentication type also have a sub-menu to set EAP fast-specific parameters:

	 If you need to use protected authentication credential, check 'Use protected authentication credential' box, and click 'Import' to load .pac credential file; to remove a loaded credential file, click 'Remove'.
Session Resumption	You can enable or disable session resumption here. If you don't know if you should enable session resumption or not, please ask your 802.1x authentication administrator.
ID \ Password tab	Input 802.1x username (ID) and password and other information if it is required here. Click 'Show Password' to show the password you typed.
Client Certification tab	Use this tab to select a local certificate from dropdown menu. If the access point you wish to connect required a specific client certificate, the certificate must be installed on your computer, and you can select the certificate here.
Server Certification tab	Use this tab to use server-based certification. Please select a CA (Certificate Authority) from dropdown menu. If intermediate certificates are allowed, please select 'Allow intermediate certificates'. Also, if you need to specify CA server's name, you can specify it in 'Server name' field. You can select 'Server name must match', so the CA server's name must be the same with the value you set in 'Server name' field; If only the domain name part of full server name must the same with the value you set in 'Server name' field, select 'Domain name must end in specified name'.

After you complete all information related to the access point, click ‘OK’ to save the profile, or click ‘cancel’ to cancel adding a new profile.

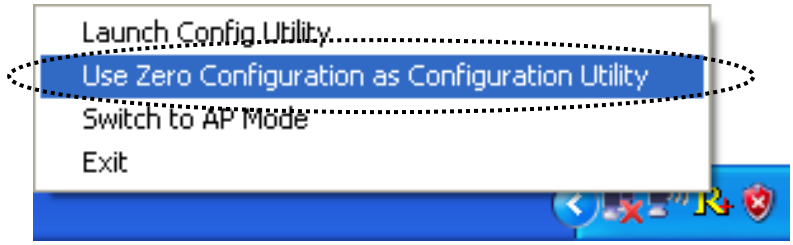
If the profile is created, you will see the information in the Profile List.



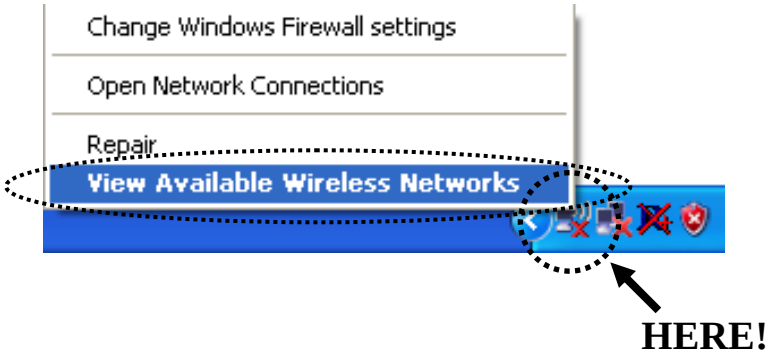
2-2-2 Using Windows Zero Configuration

Windows XP and Vista has a built-in wireless network configuration utility, called as ‘Windows Zero Configuration’ (WZC). You can also use WZC to configure your wireless network parameter:

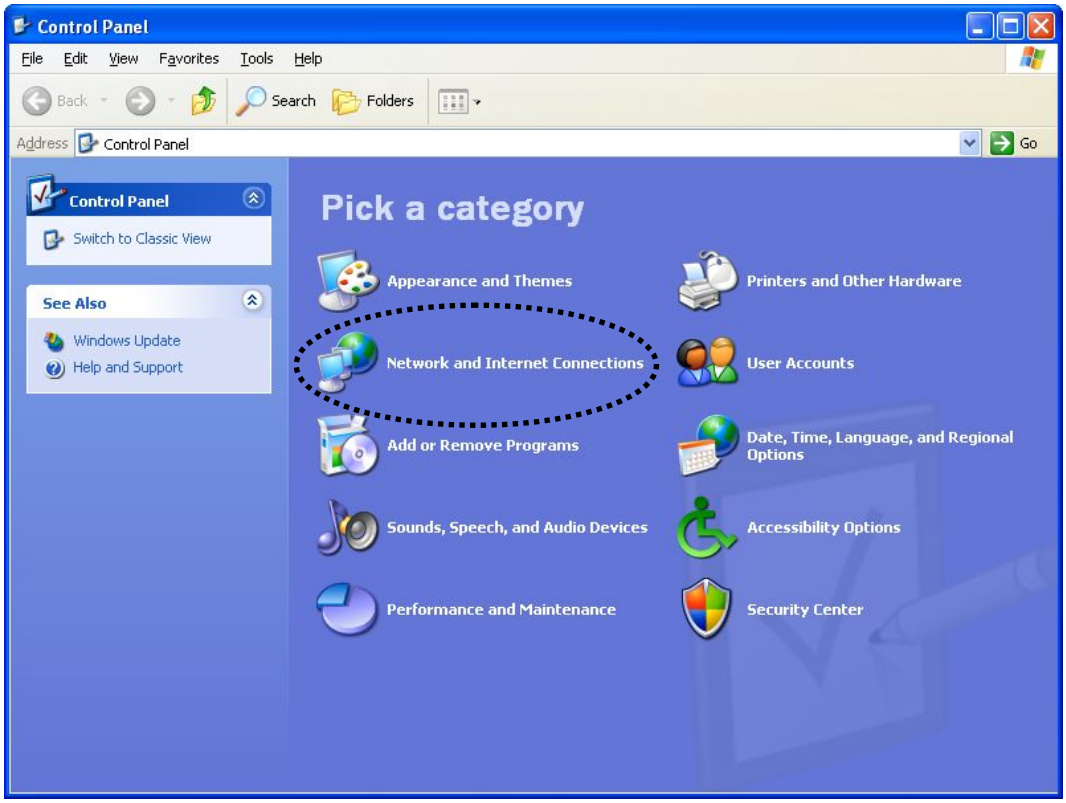
1. Right-click Ralink configuration utility icon and select ‘Use Zero Configuration as Configuration utility’.



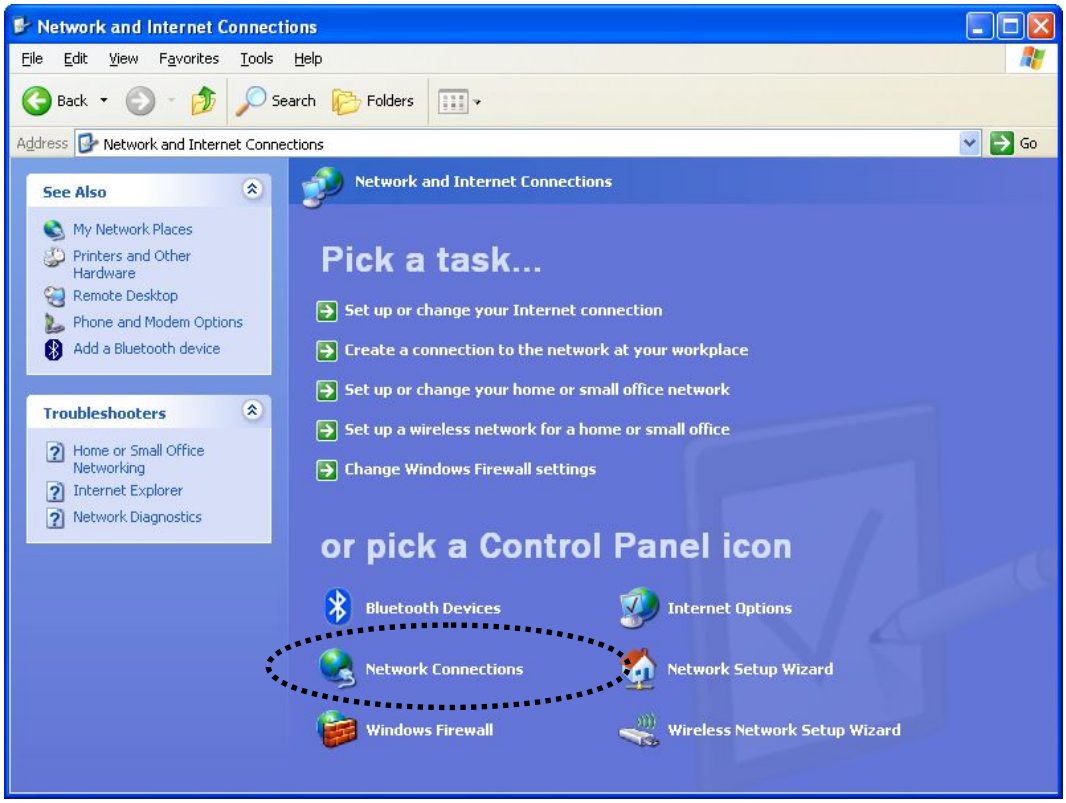
2. Right click Windows Zero Configuration icon and select ‘View Available Wireless Networks’. If you can not find the icon, please follow the procedures from step 3 to step 5.



3. Click ‘Start’ button (should be located at the bottom-left corner of windows desktop), click ‘Control Panel’, then click ‘Network and Internet Connections’ in Control Panel.

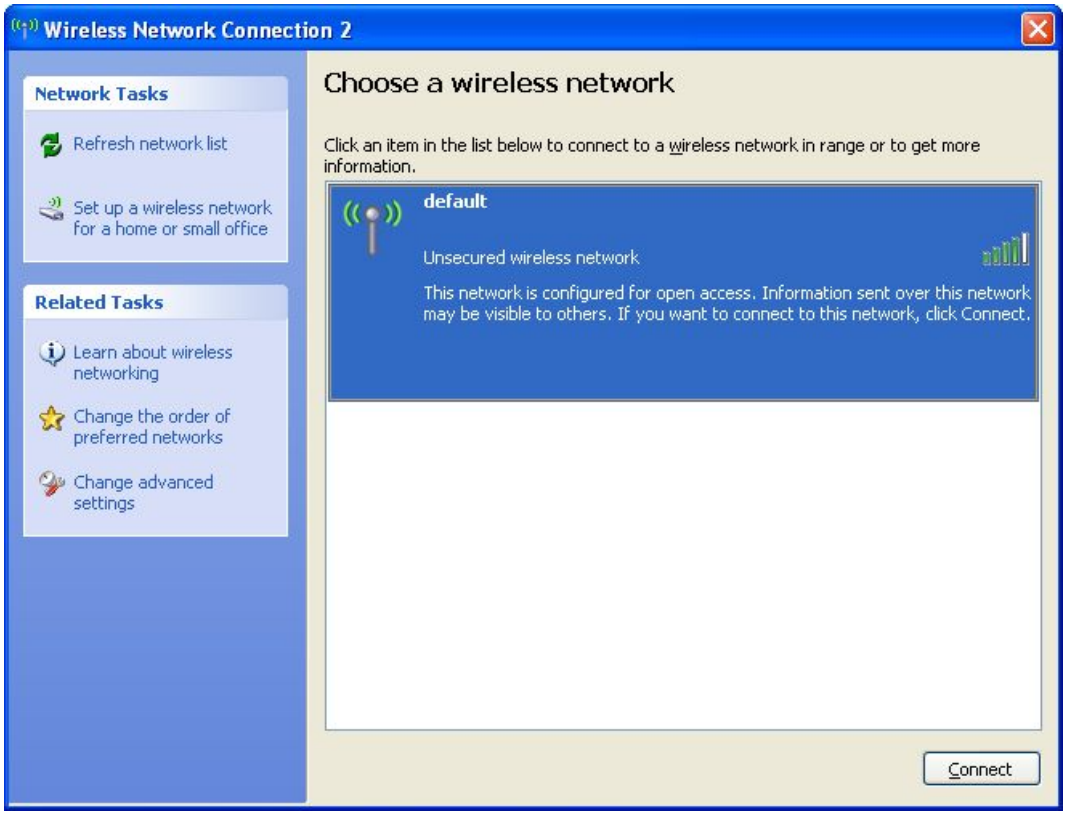


4. Click ‘Network Connections’.


Network and Internet Connections
File Edit View Favorites Tools Help
Back Search Folders
Address Network and Internet Connections
Go
See Also
My Network Places
Printers and Other Hardware
Remote Desktop
Phone and Modem Options
Add a Bluetooth device
Troubleshooters
Home or Small Office Networking
Internet Explorer
Network Diagnostics
Network and Internet Connections
Pick a task...
Set up or change your Internet connection
Create a connection to the network at your workplace
Set up or change your home or small office network
Set up a wireless network for a home or small office
Change Windows Firewall settings
or pick a Control Panel icon
Bluetooth Devices
Internet Options
Network Connections
Network Setup Wizard
Windows Firewall
Wireless Network Setup Wizard

5. Right-click ‘Wireless Network Connection’ (it may have a number as suffix if you have more than one wireless network card, please make sure you right-click the ‘Ralink 802.11n Wireless LAN Card), then select ‘View Available Wireless Networks’.

6. All wireless access points in proximity will be displayed here. If the access point you want to use is not displayed here, please try to move your computer closer to the access point, or you can click ‘Refresh network list’ to rescan access points. Click the access point you want to use if it’s shown, then click ‘Connect’.

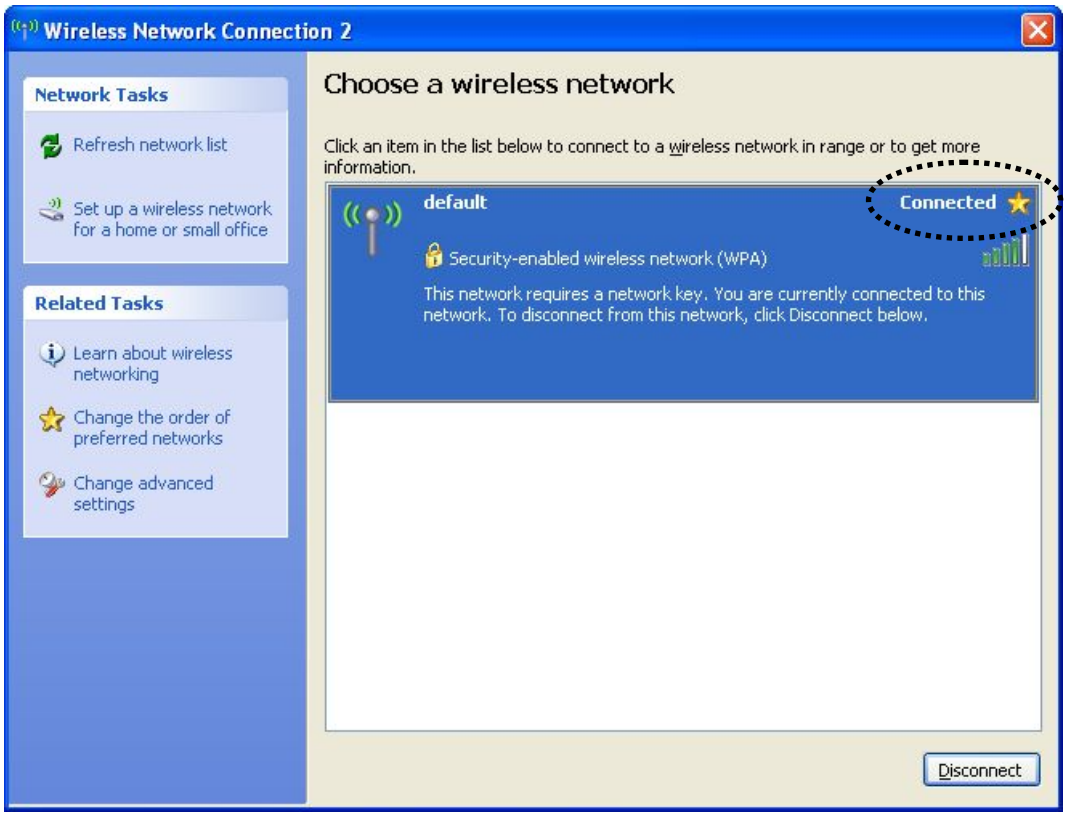

Wireless Network Connection 2
Network Tasks
Refresh network list
Set up a wireless network for a home or small office
Related Tasks
Learn about wireless networking
Change the order of preferred networks
Change advanced settings
Choose a wireless network
Click an item in the list below to connect to a wireless network in range or to get more information.
default
Unsecured wireless network
This network is configured for open access. Information sent over this network may be visible to others. If you want to connect to this network, click Connect.
Connect

7. If the access point is protected by encryption, you have to input its security key or passphrase here. It must match the encryption setting on the access point.

   If the access point you selected does not use encryption, you'll not be prompted for security key or passphrase.

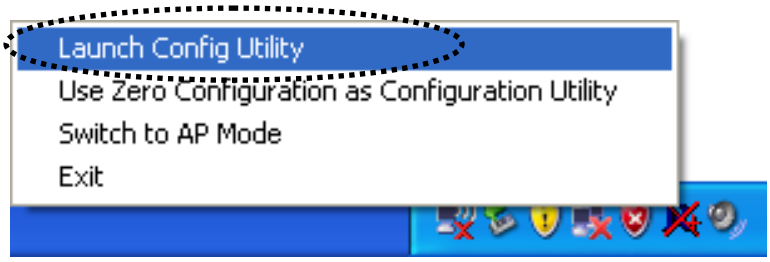
Wireless Network Connection
The network 'default' requires a network key (also called a WEP key or WPA key). A network key helps prevent unknown intruders from connecting to this network.
Type the key, and then click Connect.
Network key:
Confirm network key:
Connect
Cancel

8. If you can see 'Connected' message, the connection between your computer and wireless access point is successfully established.

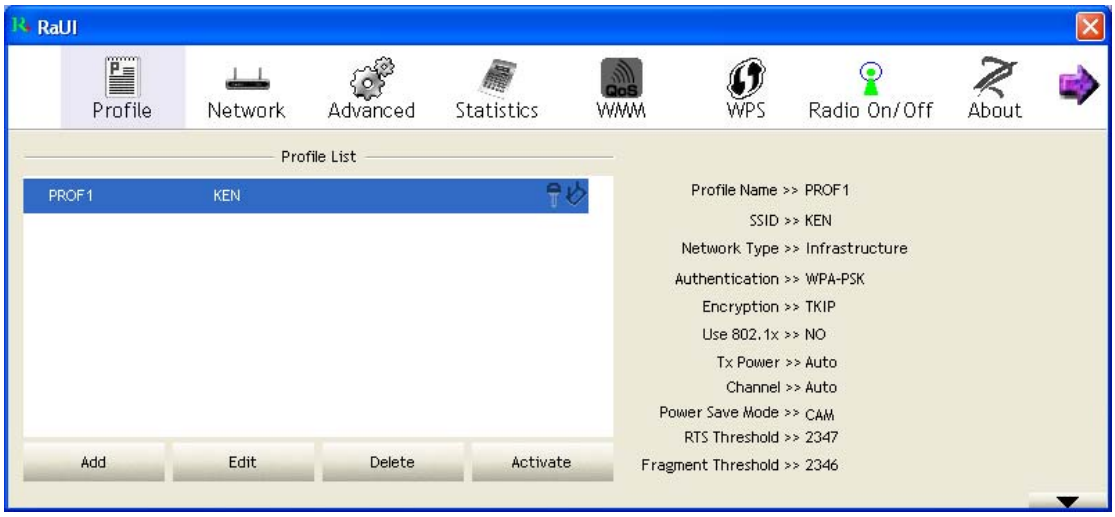

Wireless Network Connection 2
Network Tasks
Refresh network list
Set up a wireless network for a home or small office
Related Tasks
Learn about wireless networking
Change the order of preferred networks
Change advanced settings
Choose a wireless network
Click an item in the list below to connect to a wireless network in range or to get more information.
default
Connected
Security-enabled wireless network (WPA)
This network requires a network key. You are currently connected to this network. To disconnect from this network, click Disconnect below.
Disconnect

2-3 Profile Management

If you need to connect to different wireless access points at different time, like of access point of your home, office, cybercafe, or public wireless service, you can store the connection parameters (encryption, passphrase, security etc, etc.) as a profile for every access point, so you don't have to input these parameters every time when you want to connect to a specific wireless access point. To manage profiles, right-click the Ralink configuration utility icon located at lower-right corner of computer desktop, then click 'Launch Config Utility'.

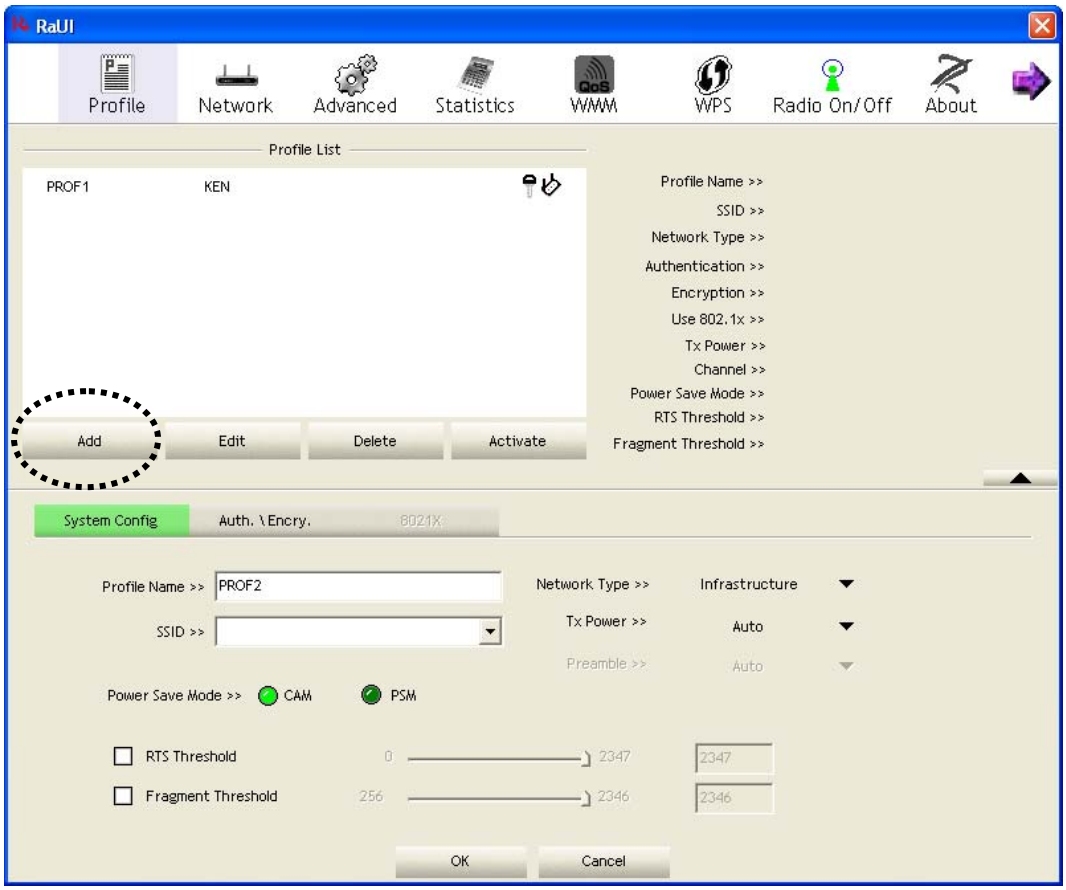


Click the 'Profile' menu. All profiles will be listed in 'Profile List', and you can select a profile from the list, all information about selected profile will be listed.



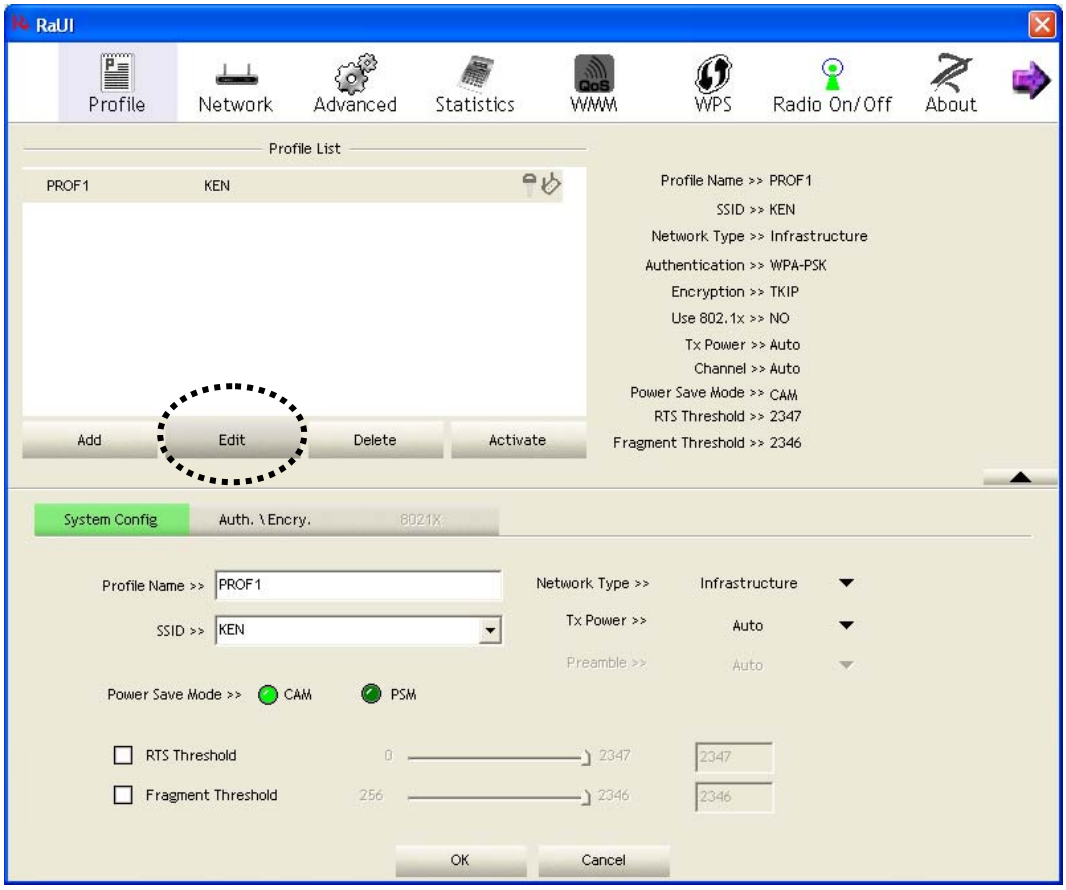
2-3-1 Add a profile

If you want to click new profile, click ‘Profile’ menu, then click ‘Add’ button. You’ll be prompted to input detailed information of access point, as described in Section 2-2-1-3.



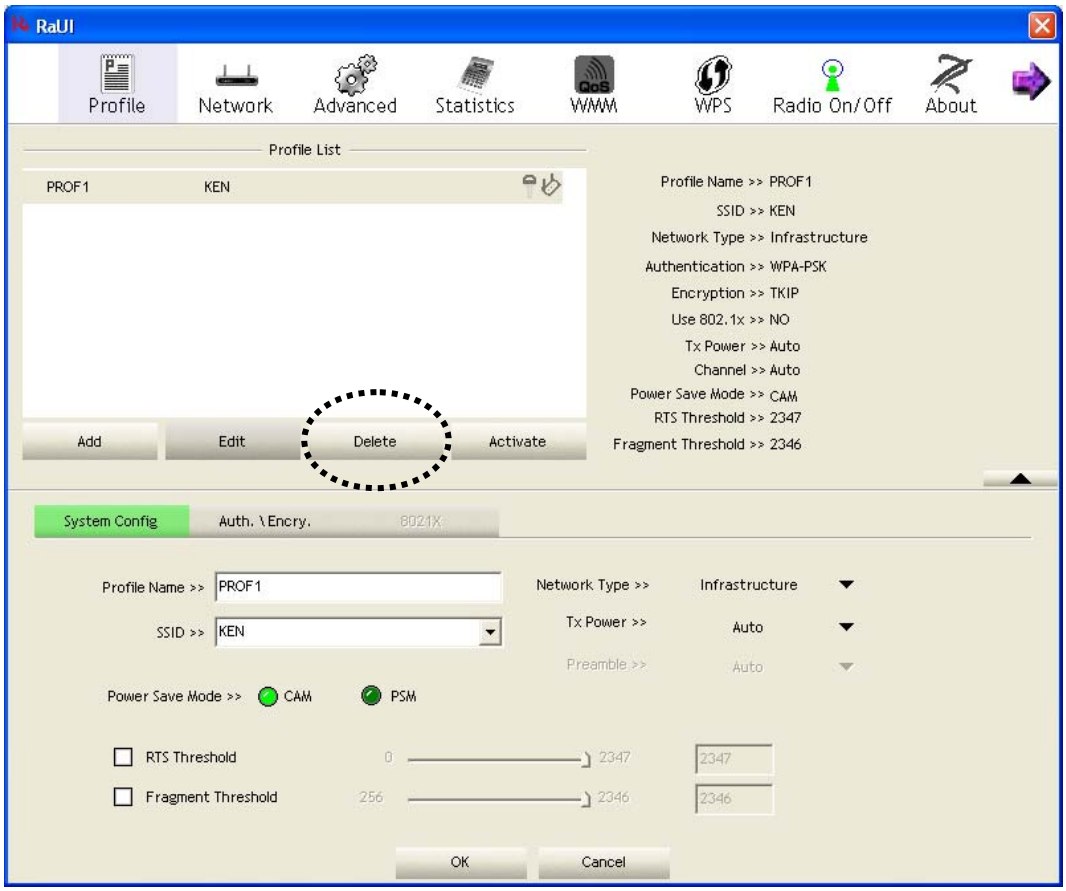
2-3-2 Edit an existing profile

If you have added a profile before, and you wish to change the content of the profile, you can use this function. Please select a profile from the list first, then click ‘Edit’ button. You’ll be provided with the contents of selected profile, and you can edit them. Click ‘OK’ to save changes, or click ‘Cancel’ to discard changes.



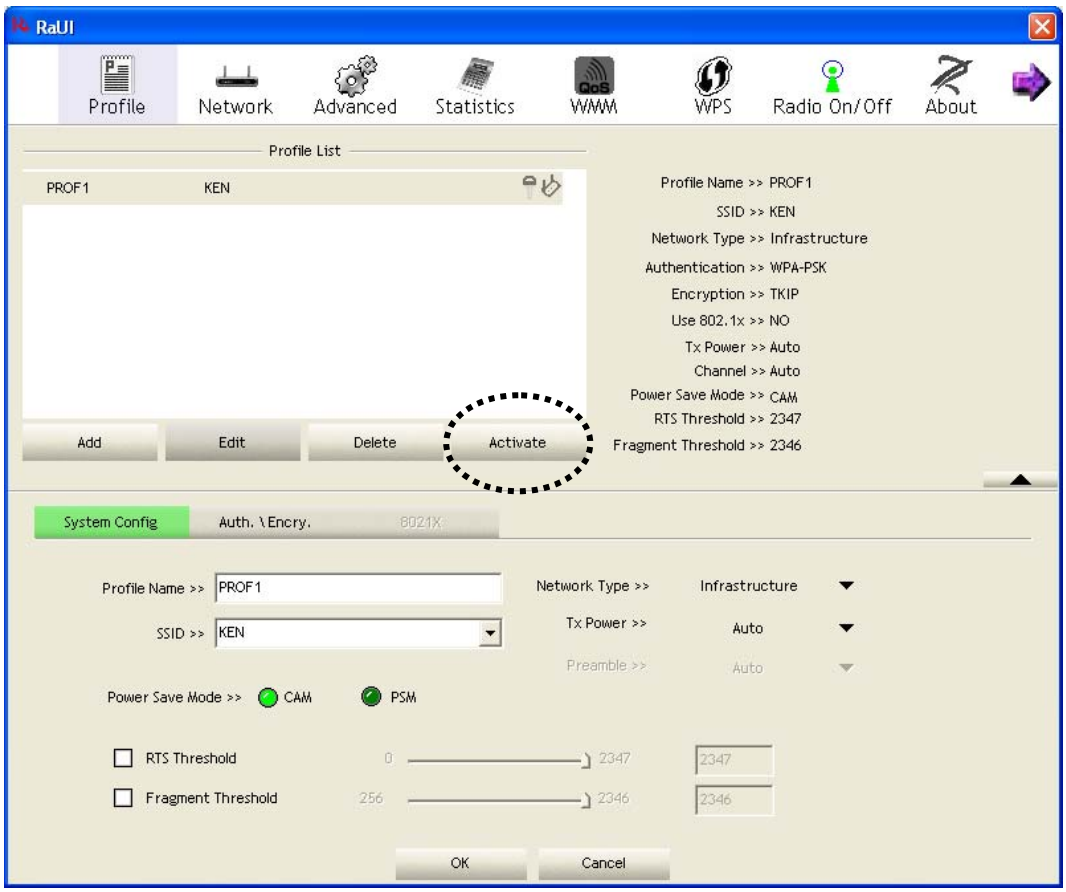
2-3-3 Delete an existing profile

If you no longer need a profile, you can delete it. Select the profile you wish to delete from the list, and click ‘Delete’ button to delete it.



2-3-4 Activate a profile

When you want to connect to a specific wireless device in the profile list, you can select it and click ‘Activate’ button, to establish connection with it.



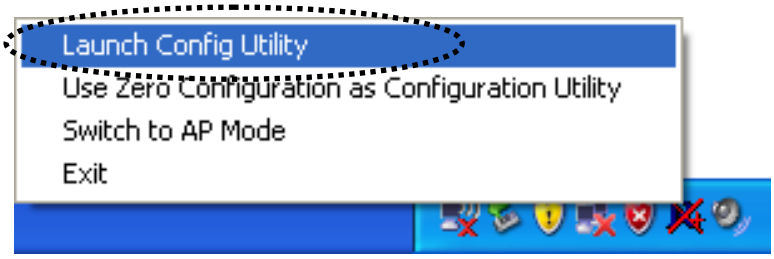
When you selected a profile and click ‘Activate’ button to activate the profile, a ▶ icon will be displayed in front of the profile to show that the connection is failed; When the connection is successfully established, a ▶ icon will be displayed.

2-4 Advanced Settings

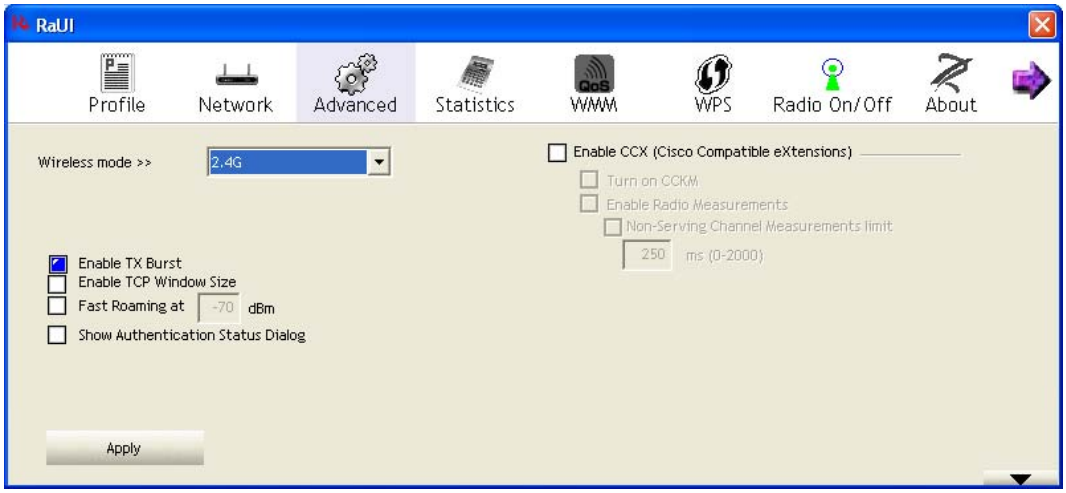
This wireless network card provides several advanced settings for experienced wireless users. You can change these settings to increase data transfer performance, or change operation mode.

Please follow the following instructions to set advanced wireless settings:

1. Right-click the Ralink configuration utility icon located at lower-right corner of computer desktop and then click ‘Launch Config Utility’.



2. Click ‘Advanced’ menu, and the following settings will appear:



Here are descriptions of every setup item:

Item Name	*Description*
Wireless mode	Display the wireless operation mode of the network card.
Enable Tx Burst	Check this box to accelerate the data transmit rate. It may not work with all wireless access point and wireless devices.
Enable TCP Window Size	Check this box and the configuration utility will adjust TCP window size automatically to get better performance. It should be safe for most of wireless environments, but if you found some problem on data transfer, uncheck this box.
Fast Roaming	Check this box and you can control the threshold that the wireless network card should switch to another wireless access point with better signal quality. Only adjust value when you understand what it means and you need to roam between multiple access points.
Show Authentication Status Dialog	When your computer is being authenticated by wireless authentication server, a dialog window with the process of authentication will appear. This function is helpful to find out the problem when you can not be authenticated, and you can provide this information to authentication server's administrator for debugging purpose.
Enable CCX	Enable Cisco Compatible eXtensions. CCX is a wireless feature developed by Cisco used to improve the wireless performance with CCX compatible wireless devices. Check this box if you need to connect to CCX-compatible wireless devices. When you enabled CCX, the following setup items will become available: Turn on CCKM: Check this box to enable CCKM (Cisco Centralized Key Management), which enables wireless clients to roam between CCKM-enabled access points in very short time.

	Enable Radio Measurements: When you're connecting to CCX-compatible access point, check this box to enable radio measurement function to improve wireless connectivity. Non-Serving Channel Measurements Limit: When you're connecting to CCX-compatible access point, check this box to enable measurement on unused radio channels to improve wireless connectivity.

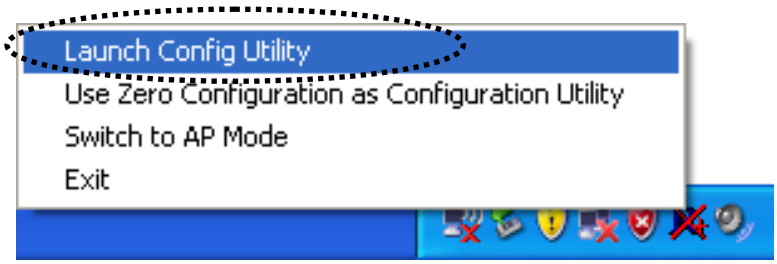
After you finish the settings, click 'Apply' to apply new settings.

2-5 View Network Statistics

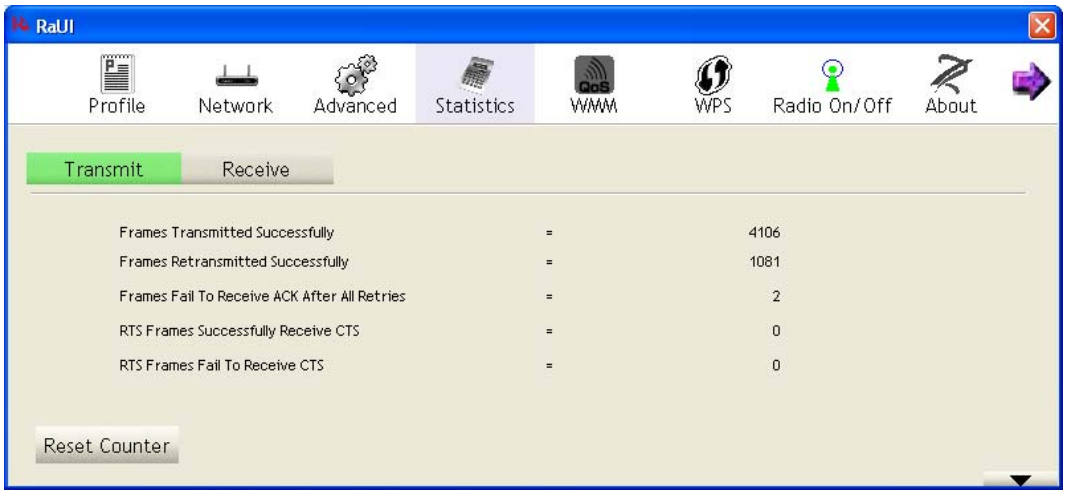
The configuration utility provides information about network statistics and link status. If you want to know how your wireless network card works, you can use these functions to get detailed information about the wireless connection you're using.

Please follow the following instructions to check network statistics:

1. Right-click the Ralink configuration utility icon located at lower-right corner of computer desktop and then click 'Launch Config Utility'.



2. Click 'Statistics' menu and the statistics of wireless connection will be displayed:



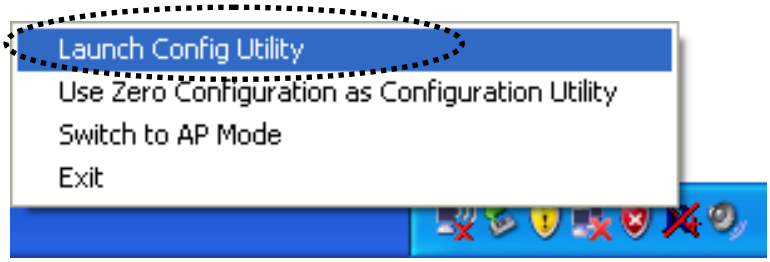
All connection-related statistics is displayed here. You can click 'Transmit' or 'Receive' tab, to view the statistics of transmitted or received packets. You can also click 'Reset Counter' button, to reset the statistics of all items back to 0.

2-6 WMM Setting

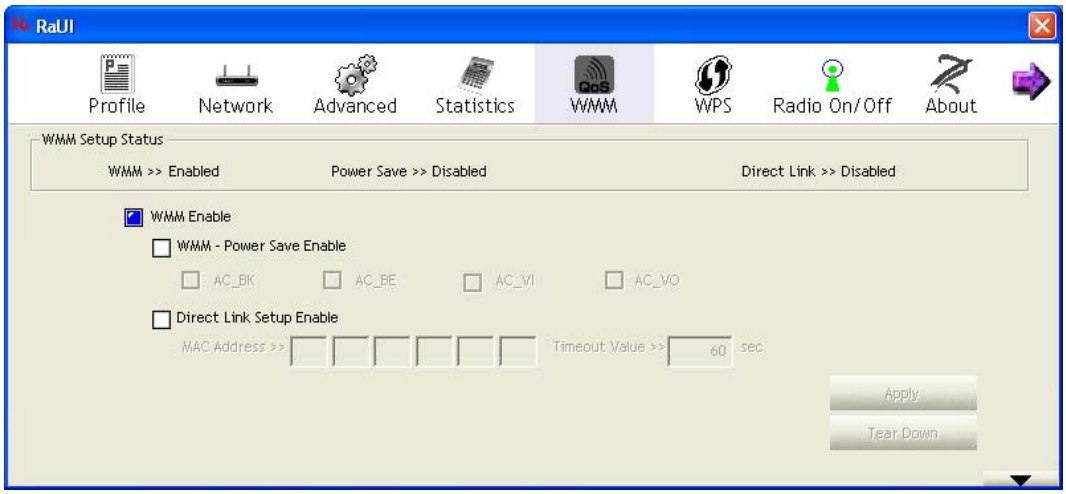
This wireless network card provides WMM (Wi-Fi Multimedia) function, which can improve the performance of certain network applications, like audio/video streaming, network telephony (VoIP), and others. When you enable the WMM function of this network card, you can define the priority of different kinds of data, to give higher priority to applications which require instant responding. Therefore you can improve the performance of such network applications.

Please follow the following instructions to set advanced wireless settings:

1. Right-click the Ralink configuration utility icon located at lower-right corner of computer desktop and then click ‘Launch Config Utility’.



2. Click ‘WMM’ menu, and the following settings will appear:



In ‘WMM Setup Status’ block, current WMM settings will be displayed. And here are descriptions of every setup item:

Item Name	*Description*
WMM Enable	Check this box to enable WMM function. Please click ‘Apply’ button on the right of this check box after you check or uncheck this box, so corresponding settings in this window will be activated or deactivated respectively.
WMM - Power Save Enable	Check this box to enable WMM power saving mode to save energy, and let your computer’s battery live longer. You also have to select WMM power save modes here: AC_BE: Best Performance AC_BK: Worst Performance AC_VI: Video data has priority AC_VO: Voice data has priority
Direct Link Setup Enable	If you have another WMM-enabled wireless device, you can enter its MAC address here, then click ‘Apply’ button, and this network card will establish a direct link to the wireless device you specified here. You also have to specify the timeout value of this directly-linked wireless device. Valid values are from 1 to 65535 (seconds), and input ‘0’ for infinity. If you want to remove a specific wireless device from direct link table, select the device and click this button to remove it.

2-7 WPS Configuration

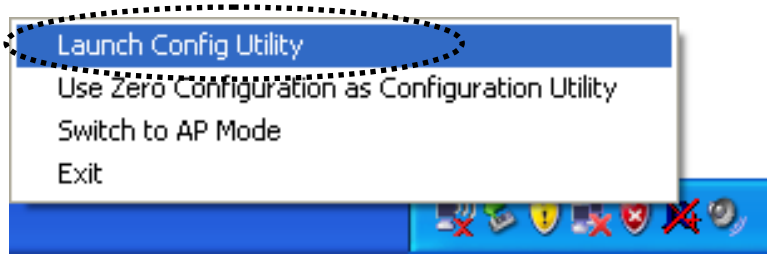
Wi-Fi Protected Setup (WPS) is the latest wireless network technology which makes wireless network setup become very simple. If you have WPS-enabled wireless access point, and you want to establish a secure connection to it, you don’t have to configure the wireless access point and setup data encryption by yourself. All you have to do is to go to the WPS setup page of this wireless card, click a button, and then press a specific button or enter a set of 8-digit code on the wireless access point you wish to establish a secure connection - just three simple steps!

For older wireless access points, it’s possible to perform a firmware upgrade to become a WPS-enabled access point. Since they may not have a hardware button to press for WPS setup, you can use an alternative WPS setup method - input the pin code. Every WPS-compatible wireless network card support pin code configuration method; you can just input the code to wireless access point, and the wireless access point and wireless network card will do the rest for you.

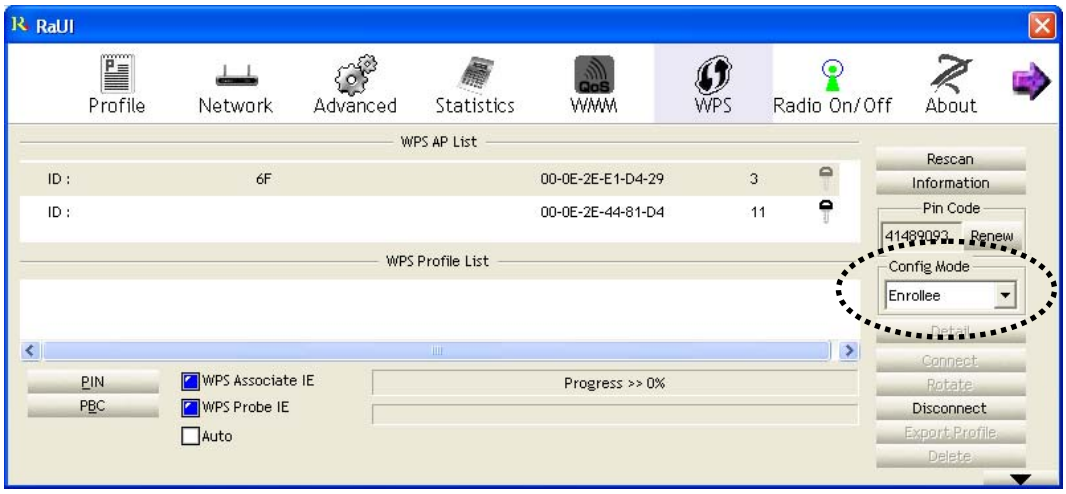
This wireless network card is compatible with WPS. To use this function, the wireless access point you wish to connect to must support WPS function too. Now, please follow the following instructions to establish secure connection between WPS-enabled wireless access point and your wireless network card.

2-7-1 WPS Setup - PBC (Push-Button Configuration)

1. Right-click the Ralink configuration utility icon located at lower-right corner of computer desktop and then click ‘Launch Config Utility’.



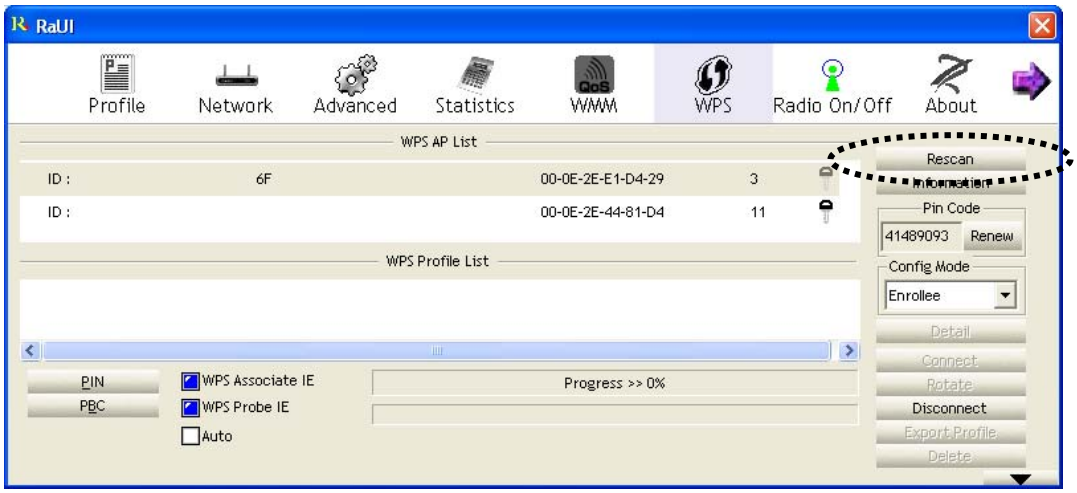
2. Click ‘WPS’ menu, and the following settings will appear.



3. Set ‘Config Mode’ to ‘Enrollee’, and then push the ‘WPS’ button on your wireless access point (the button used to activate WPS standby mode may have another name), or use other way to start WPS PBC standby mode as the instruction given by your wireless access point’s user manual.

   You can also set ‘Config Mode’ to ‘Registrar’. In this mode, this wireless network card will wait for other WPS-enabled access points to send WPS pairing requests. Please refer to the instruction given by your wireless access point’s user manual to understand how to send WPS requests.

4. Before you start to establish the wireless connection by using WPS, you can click ‘Rescan’ button to search for WPS-enabled access points near you again, to make sure the WPS function of your access point is activated.

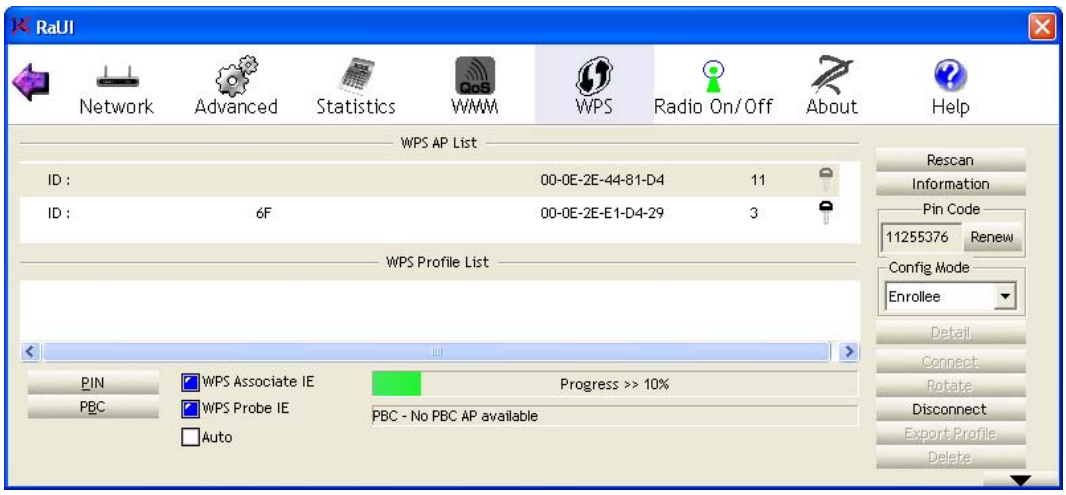


All access points with WPS function enabled will be displayed here. Please make sure the access point you wish to connect is displayed. If not, please click ‘Rescan’ few more times. You can also click ‘Information’ button to see the detailed information about selected access point.

5. Start PBC pairing procedure at access point side (please refer to the instruction given by your access point’s manufacturer), then click ‘PBC’ button in wireless configuration utility to start to establish wireless connection by WPS. Please be patient (This may require several seconds to one minute to complete). When you see ‘WPS status is connected successfully’ message, means the connection between this wireless network card and access point is successfully established by WPS, and the information about access point you connected to will be displayed.

6. You can click ‘Detail’ button to see detailed information of connected access point. If you wish to save this connection as a profile, you can click ‘Export Profile’ button, and this connection will be saved. You can find this connection in ‘Profile’ tab in a later time.

7. Sometime WPS may fail (In the following picture, WPS pairing is failed because no WPS-enabled access point is found):



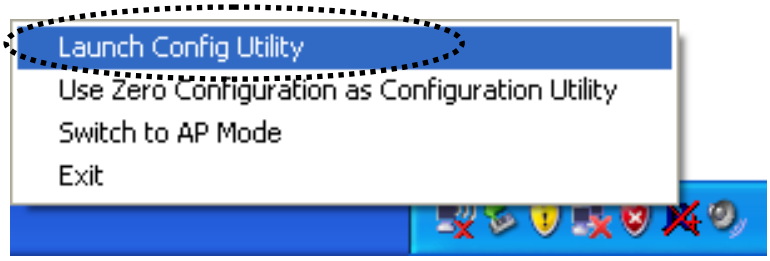
You can click ‘PBC’ button few more times to try again. When an access point is connected, you can click ‘Disconnect’ to disconnect your wireless network card from a connected access point, or select another WPS-enabled wireless access point, then click ‘Connect’ to establish connection to selected access point, if there are more than one WPS-enabled access point found. You can also click ‘Rotate’ button, and next access point on the list will be selected to establish connection.

If you want to delete a found access point from the list, select it and click ‘Delete’ button.

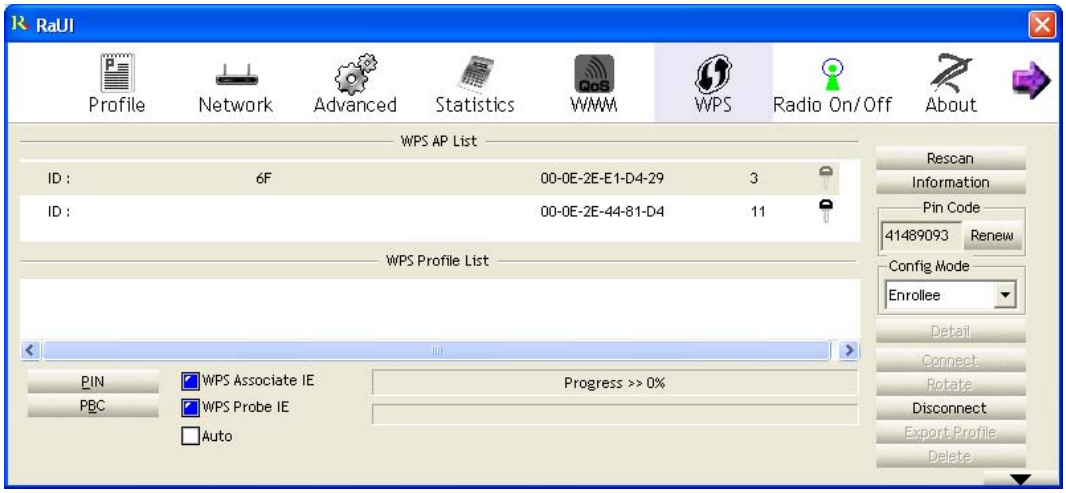
2-7-2 WPS Setup - PIN

If the wireless access point you wish to connect supports PIN, please follow the following instructions to establish connection to it:

1. Right-click the Ralink configuration utility icon located at lower-right corner of computer desktop and then click ‘Launch Config Utility’.



2. Click ‘WPS Configuration’ menu, and the following settings will appear.



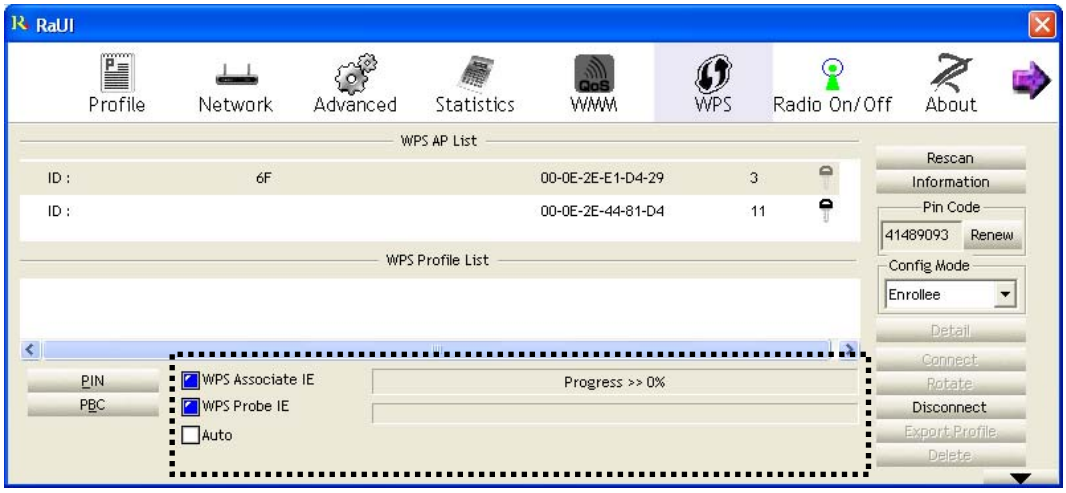
3. The PIN code of your wireless network card is an eight-digit number located at the upper-right position of configuration utility. Remember it, and input the number to your wireless access point as the WPS PIN code (Please refer to the user manual of your wireless access point for instructions about how to do this).

NOTE: If you experienced problem with the pin code provided here, you can click ‘Renew’ to get a new pin code.

4. Click ‘PIN’ button now, and wait for few seconds to one minute. If a wireless access point with correct PIN code is found, you’ll be connected to that access point.

5. You may have to click ‘PIN’ for few more times to try again. If you still can not connect to access point by this way, please make sure the PIN code you provided to access point is correct.

There are also some options available for WPS configuration:



WPS associate IE: Check this box to send the association request with WPS IE during WPS setup. This is optional and you can use default value if you don’t know what will be affected.

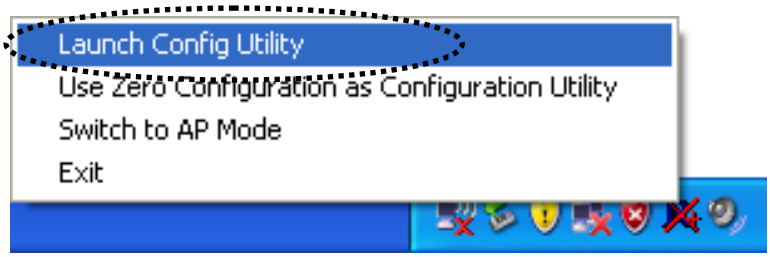
WPS probe IE: Check this box to send the WPS probe request with WPS IE during WPS setup. This is optional and you can use default value if you don’t know what will be affected.

Auto: When in PIN mode, wireless access point to be connected will be selected automatically if this box is checked.

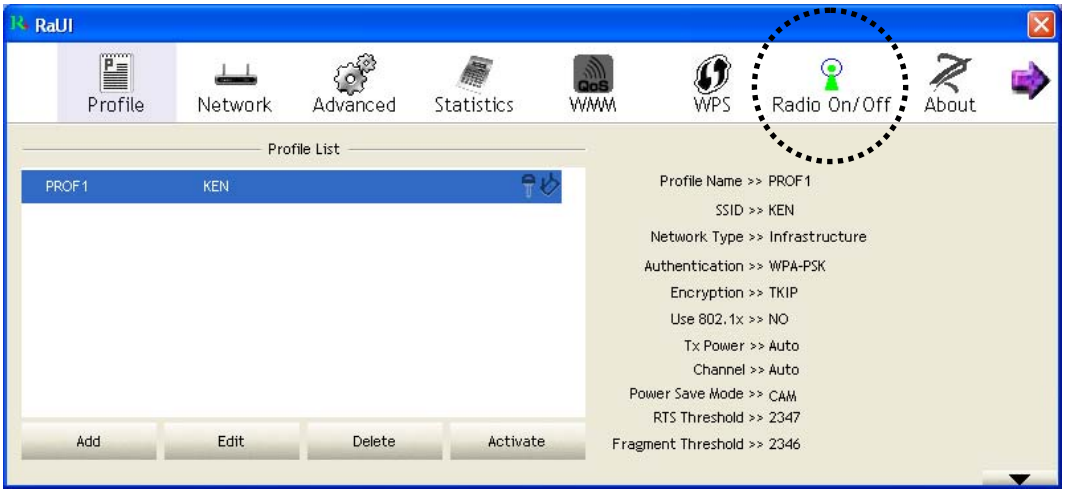
2-8 Radio On/Off

You can switch the wireless radio transceiver on and off by the utility, so if you want to disable wireless network function, you don't have to remove the network card physically.

1. Right-click the Ralink configuration utility icon located at lower-right corner of computer desktop and then click 'Launch Config Utility'.



2. To switch wireless radio on/off, please click 'Radio On/Off' button.



Wireless radio is on (Green)

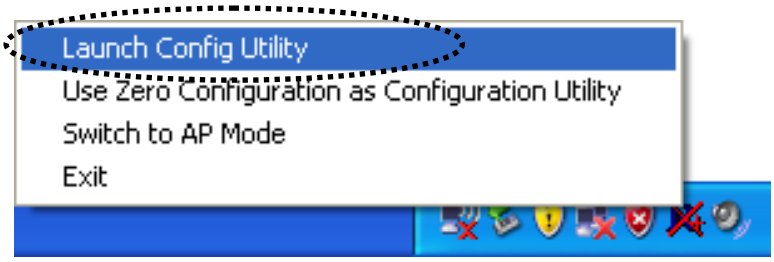
Wireless radio is off (Red)

2-9 About

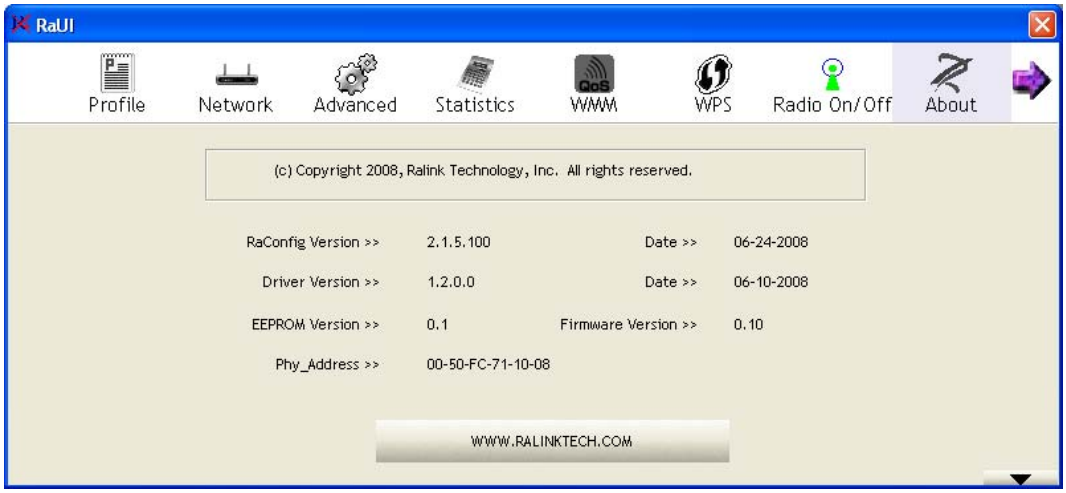
The ‘About’ tab provides you the information about version number of the configuration utility, driver, and other important information about your wireless network card.

Please follow the following instructions to see these information:

1. Right-click the Ralink configuration utility icon located at lower-right corner of computer desktop and then click ‘Launch Config Utility’.



2. Click ‘About’ tab, and the following information will appear.



2-10 On-line Help

If you need to know the directions of how to use specific function in the utility, please click ‘Help’ button. On-line help documents will be presented in Windows help format.

Click this button to view on-line help documents.

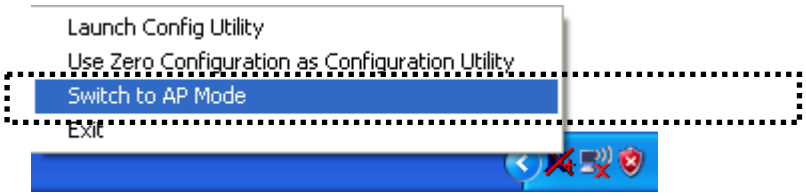
CHAPTER III: Soft-AP Function

Excepting become a wireless client of other wireless access points, this wireless card can act as a wireless service provider also! You can switch this wireless card's operating mode to 'AP' mode to simulate the function of a real wireless access point by software, and all other computers and wireless devices can connect to your computer wirelessly, even share the internet connection you have!

Please follow the instructions in following chapters to use the AP function of your wireless card.

3-1 Switch to AP Mode and Basic Configuration

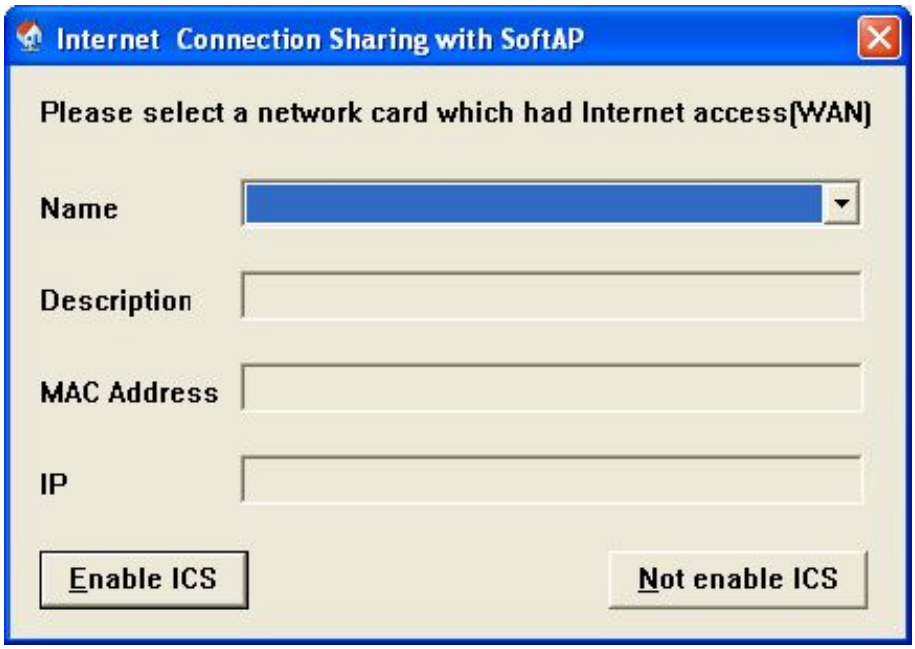
The operating mode of the wireless card is 'Station Mode' (becoming a client of other wireless access points) by default. If you want to switch to AP mode, please right-click Ralink utility icon, and select 'Switch to AP Mode'.



After you select 'Switch to AP Mode', the Ralink utility icon will be changed to:

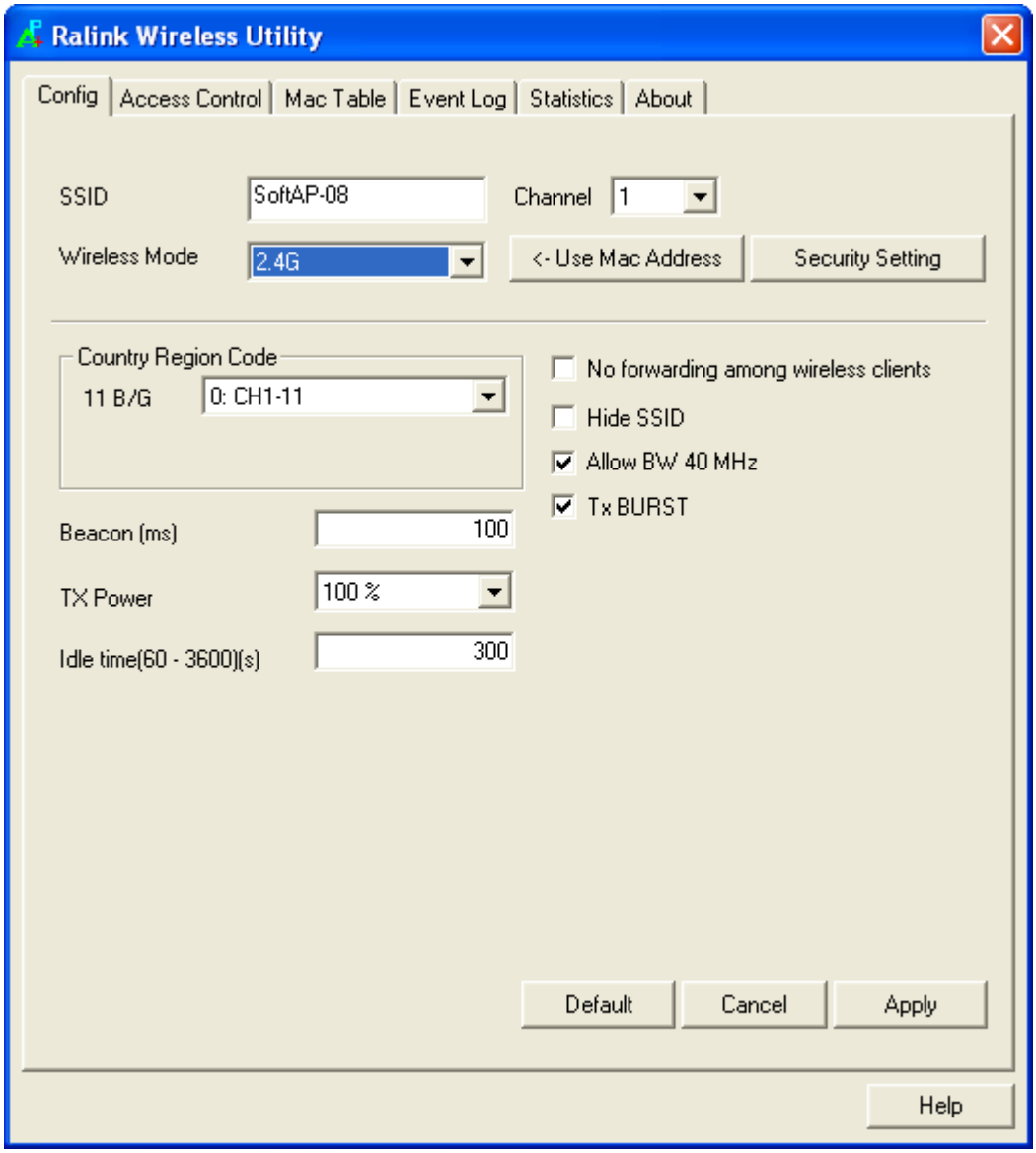
Which indicated the wireless card is operating in AP mode now. If you want to switch the wireless card back to station mode (become a client of other wireless access points), click 'Switch to Station Mode'.

A configuration window will appear after you switch the operation mode to ‘AP’, which asks you to assign an existing network card with internet connection.



If your computer has another network card which is connected to Internet, please select it from ‘Name’ dropdown menu, and click ‘Enable ICS’; if your computer does not have another network card with Internet connection, please click ‘Not enable ICS’.

After you click ‘Enable ICS’ or ‘Not enable ICS’, you’ll see the basic configuration menu of the AP function.



Here are descriptions of every setup item:

Item Name	*Description*
SSID	Please input the SSID (the name used to identify this wireless access point) here. Up to 32 numerical characters can be accepted here, excepting space.
Channel	Please select the wireless channel you wish to use. The number of channels available here will vary depends on the setting of 'Country Region Code'.
Wireless Mode	Select the operation mode of the access point here.
Use Mac Address	Click this button to use the MAC address of the

	wireless card as SSID. A prefix ‘AP’ will be added automatically.
Security Setting	Set the security options (wireless data encryption). Please refer to chapter 3-2 ‘Security Settings’ for details.
Country Region Code	Please select the country code of the country or region you live. Available options are 0-7, which will affect the available wireless channels you can use: 0: FCC (US, Canada, and other countries uses FCC radio communication standards) 1: ETSI (Europe) 2: SPAIN 3: FRANCE 4: MKK 5: MKKI (TELEC) 6: ISERAL (Channel 3 to 9) 7: ISERAL (Channel 5 to 13) **Please note that only change the country code if you are in different country. For example: when operating this product in US, only channels 1~11 can be operated. Selection of other channels is not permitted under FCC regulations.**
No forwarding among wireless clients	Check this box and wireless clients will not be able to share data with each other.
Hide SSID	Check this box and the SSID will not be broadcasted to the public. Your wireless clients must know the exact SSID to be able to connect to your computer. This option is useful to enhance security level.
Allow BW 40 MHz	Check this box to allow BW 40MHz capability.
Tx BURST	Check this box to accelerate the data transmit rate. It may not work with all wireless access point and wireless devices.

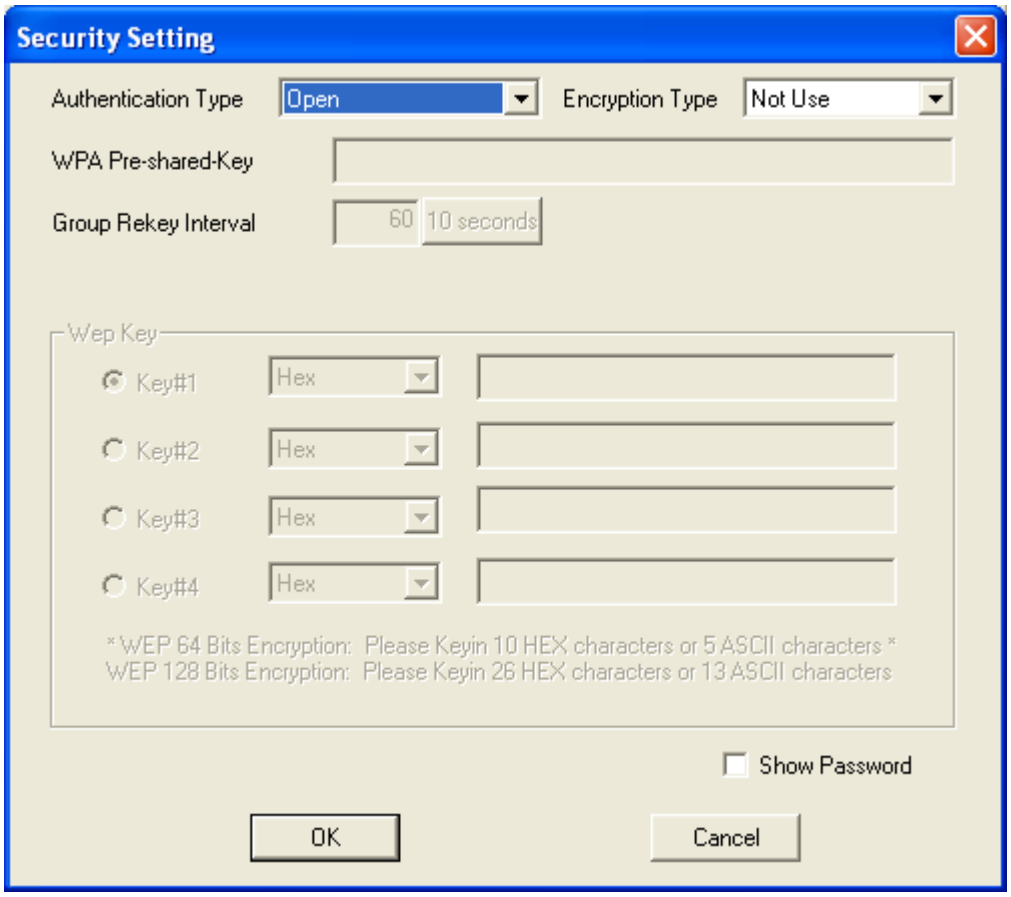
Beacon(ms)	You can define the time interval that a beacon signal should be send. Default value is 100. Do not modify this value unless you know what will be affected.
TX Power	You can select the wireless output power here. Please select a proper output power setting according to your actual needs. You may not need 100% of output power if other wireless clients are not far from you.
Idle Time	Select the idle time for the wireless access point. Default value is 300. Do not modify this value unless you know what will be affected.

To save changes, click ‘Apply button. Or you can click ‘Default’ to reset all values to factory default value.

3-2 Security Setting

This wireless card supports wireless encryption in AP mode, which will encrypt the data being transferred over the air to enhance data security level. It's recommended to enable data encryption unless you wish to open your computer (and its internet connection) to the public.

When you click 'Security Setting' in the utility, the following window will appear:



Here are descriptions of every setup item:

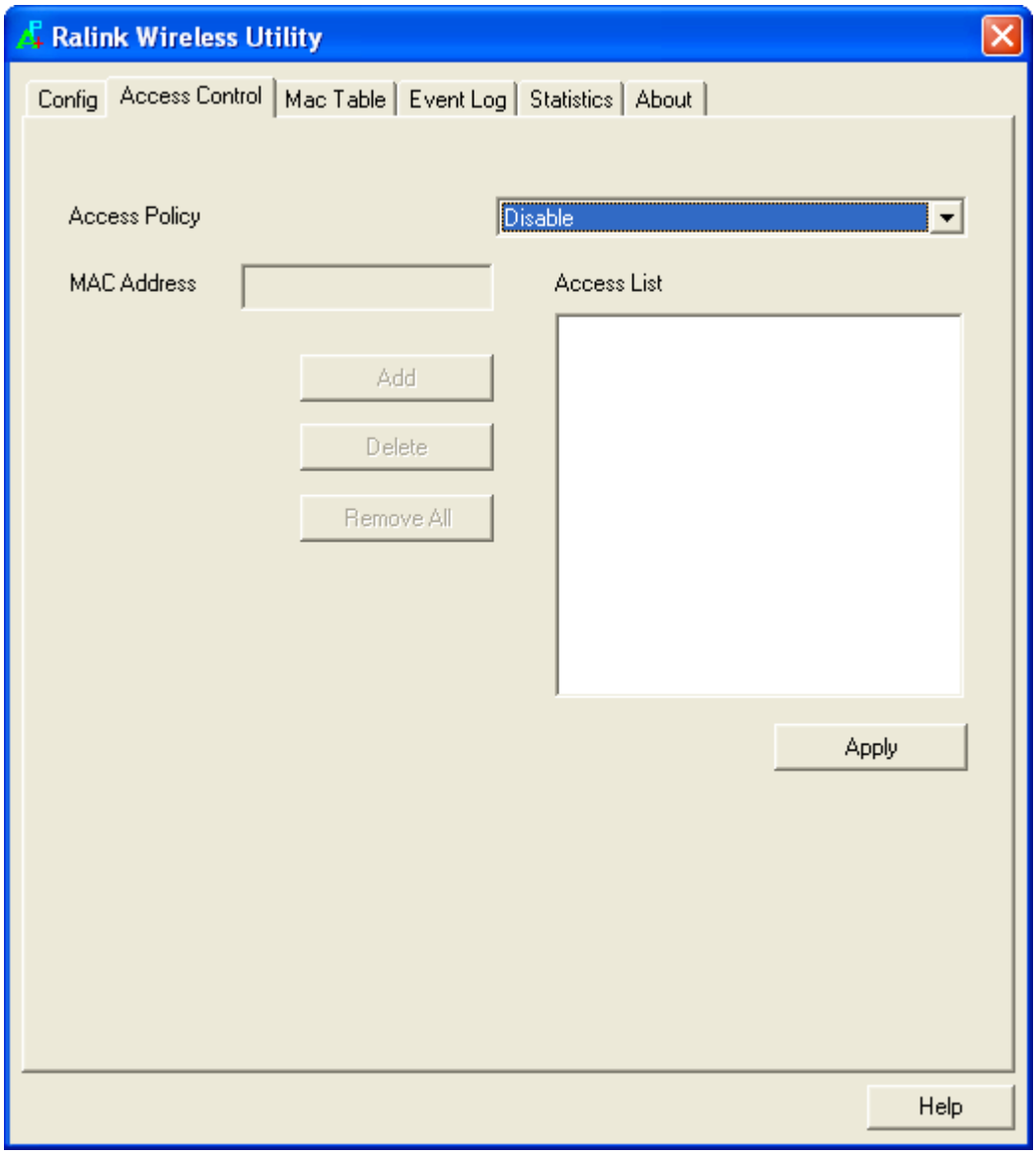
Item Name	*Description*
Authentication Type	Please select a wireless authentication type you wish to use. Available options are ‘Open’, ‘Shared’, WPA-PSK’, ‘WPA2-PSK’, and ‘WPA-PSK / WPA2-PSK’. If you want to disable wireless data encryption, you must select ‘Open’.
Encryption Type	Please select an encryption mode. The available options in this setting item will vary depending on the authentication type you select. If you select ‘Not Use’, data will not be encrypted and people with some networking knowledge will be able to read the data you transfer with proper tool.
WPA Pre-shared Key	Please input the WPA pre-shared key here. Only clients with the same pre-shared key you inputted here will be able to connect to your computer. This setting is only available when you select one of WPA encryptions.
Group Rekey Interval	You can specify the time interval to re-issue the key to your wireless clients here. You can click the button ’10 seconds’ or ‘Kpackets’ to change the unit of time interval. (every 10 seconds or a thousand data packets times the value you specified in ‘Group Rekey Interval’ field).
Wep Key	Please input the WEP encryption key here when you select ‘WEP’ as encryption type. There are 2 types of WEP key: Hex (number 0 to 9, and ASCII characters A to F) and ASCII (all alphanumerical characters plus symbols). Please select the type of WEP key first, and then input the WEP key according to the type of WEP key you selected. If you want to use WEP 64 bits encryption, please input 10 characters if you select HEX, or input 5 characters if you select ASCII. If you want to use WEP 128bits encryption, please input 26 characters if you select HEX, or input 13

	characters if you select ASCII. 128 bits encryption is safer then 64 bits, but the data transfer speed will be slightly reduced.
Show Password	Check this box and the WPA pre-shared key or WEP key you inputted will be shown, but not replaced by asterisk (*).

When you finish with setting and want to save changes, click ‘OK’ button, or click ‘Cancel’ button to discard all changes you made.

3-3 Access Control

If you’re not going to open your computer and wireless resources to the public, you can use MAC address filtering function to enforce your access control policy, so only wireless clients with MAC address you defined by this function can be connected to your software access point.



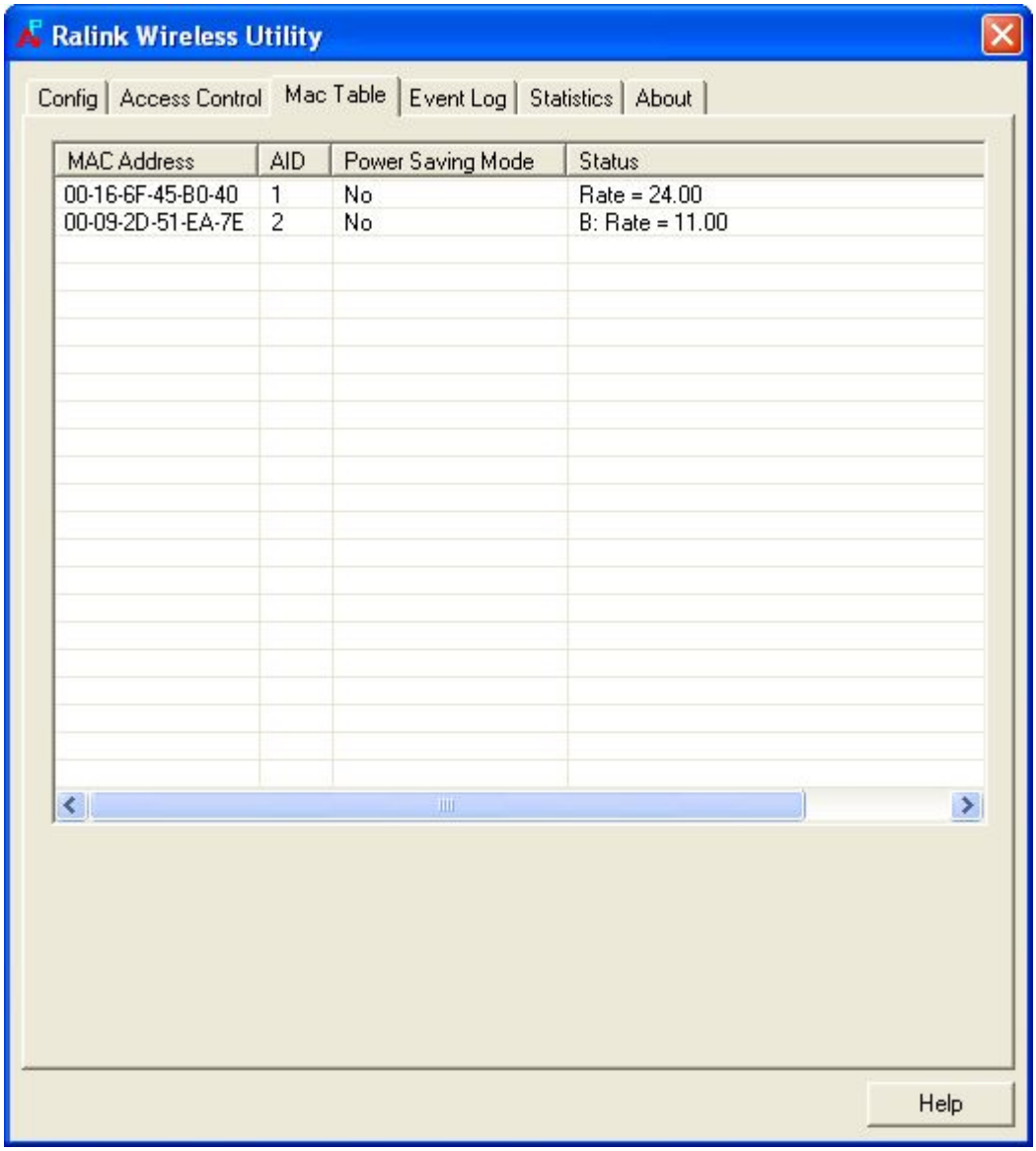
Here are descriptions of every setup item:

Item Name	*Description*
Access Policy	Select the policy type of your access rule. Disable: Allow any wireless client with proper authentication settings to connect to this access point. Allow All: Only allow wireless clients with MAC address listed here to connect to this access point. Reject All: Reject wireless clients with MAC address listed here to be connected to this access point.
MAC address	Input the MAC address of the wireless client you wish to allow or reject here. No colon (:) or hyphen (-) required.
Add	Add the MAC address you inputted in ‘MAC address’ field to the list.
Delete	Please select a MAC address from the list, then click ‘Delete’ button to remove it.
Remove All	Delete all MAC addresses in the list.

When you finish with setting and want to save changes, click ‘Apply’ button.

3-4 Connection Table

If you want to see the list of all wireless clients connected to this access point, please select ‘Mac Table’ tab from the utility.

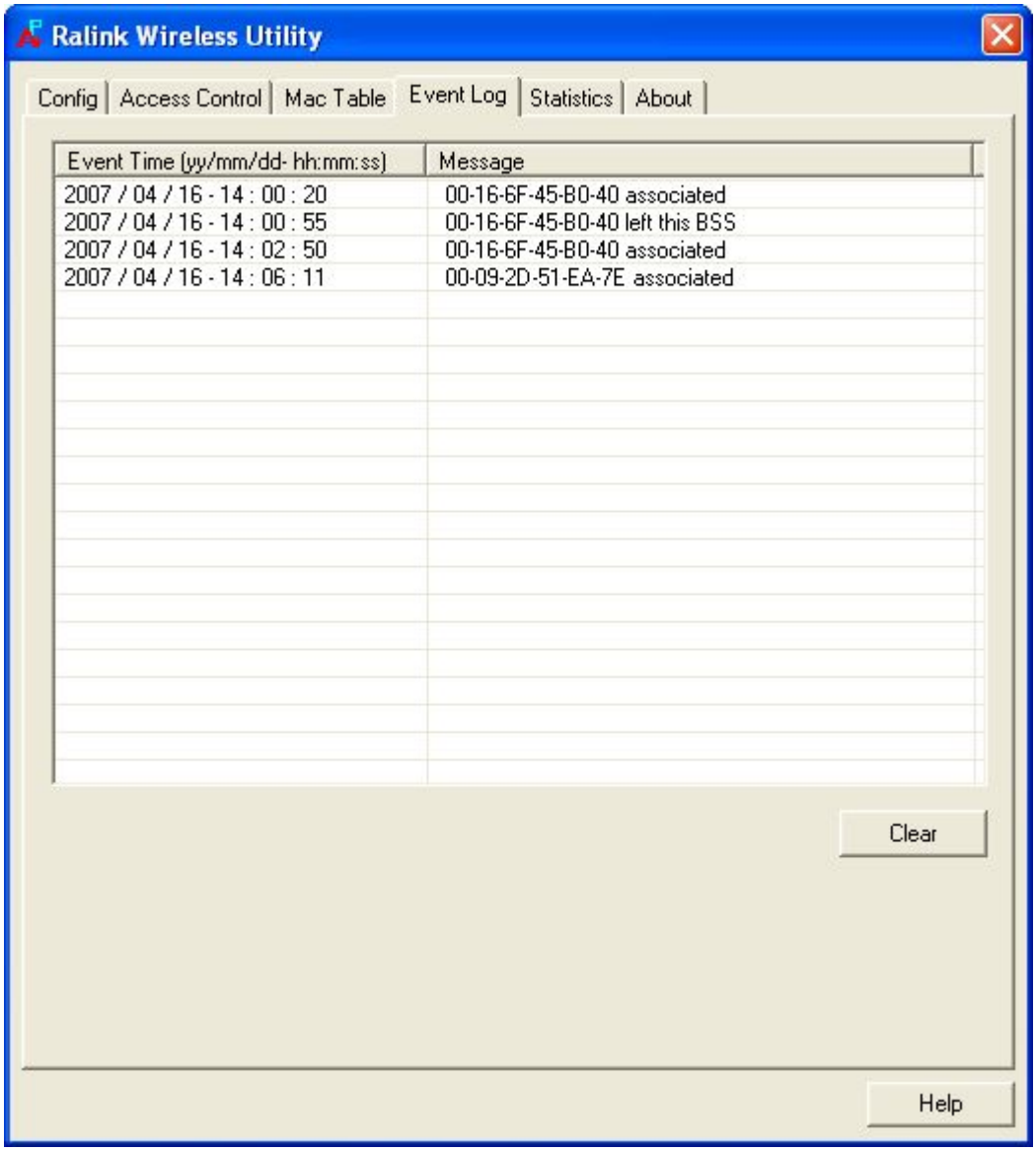


Here are descriptions of every field:

Item Name	*Description*
MAC Address	Displays the MAC address of this wireless client.
AID	The serial number of this wireless connection.
Power Saving Mode	Displays the capability of power-saving function of this wireless client.
Status	Displays additional information of this wireless Connection, like current wireless operating mode and data transfer rate.

3-5 Event Log

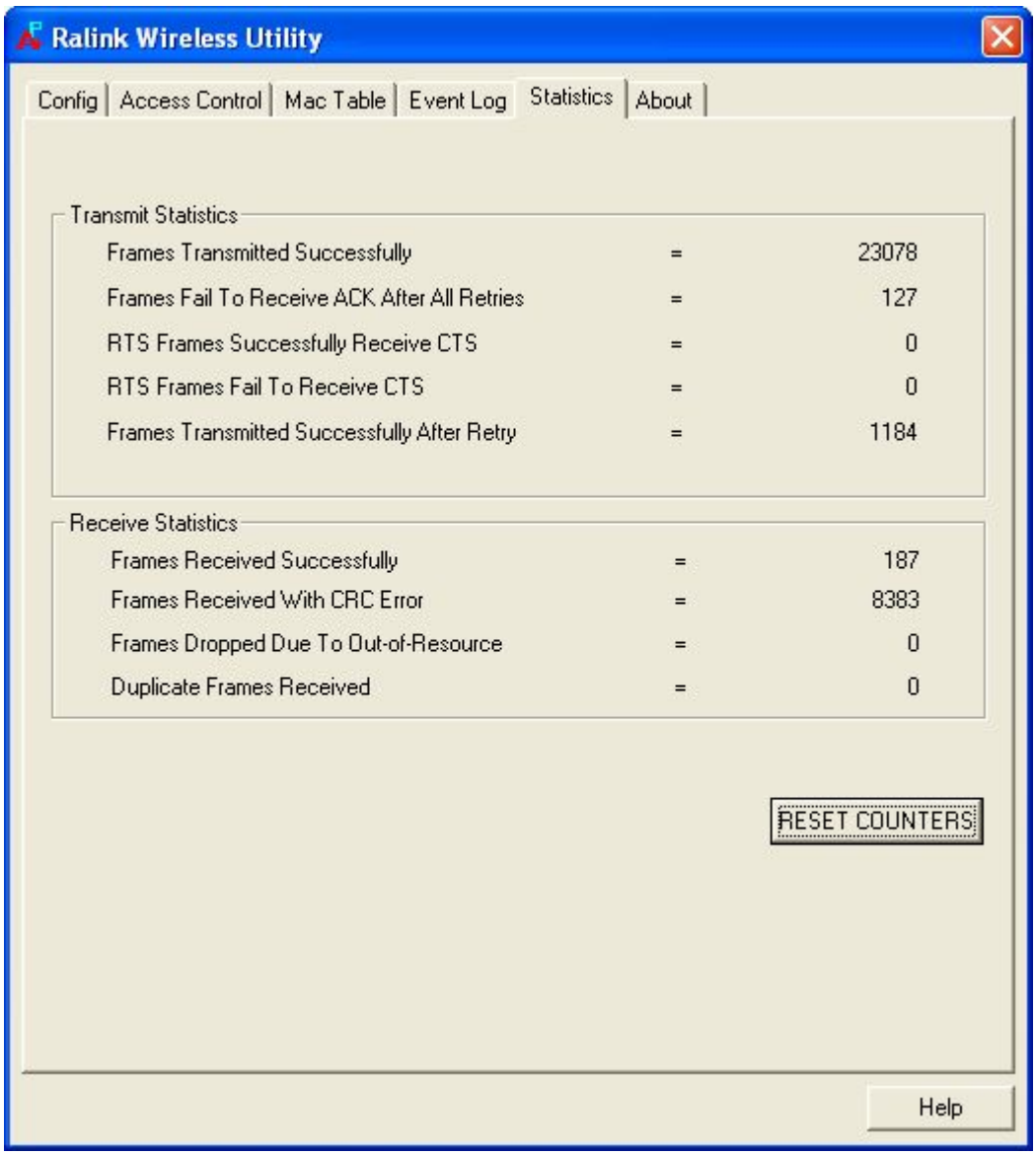
This software access point will log all wireless-related activities as a log. Click ‘Event Log’ tab, and the event log will be displayed.



You can click ‘Clear’ to remove all entries in the log.

3-6 Statistics

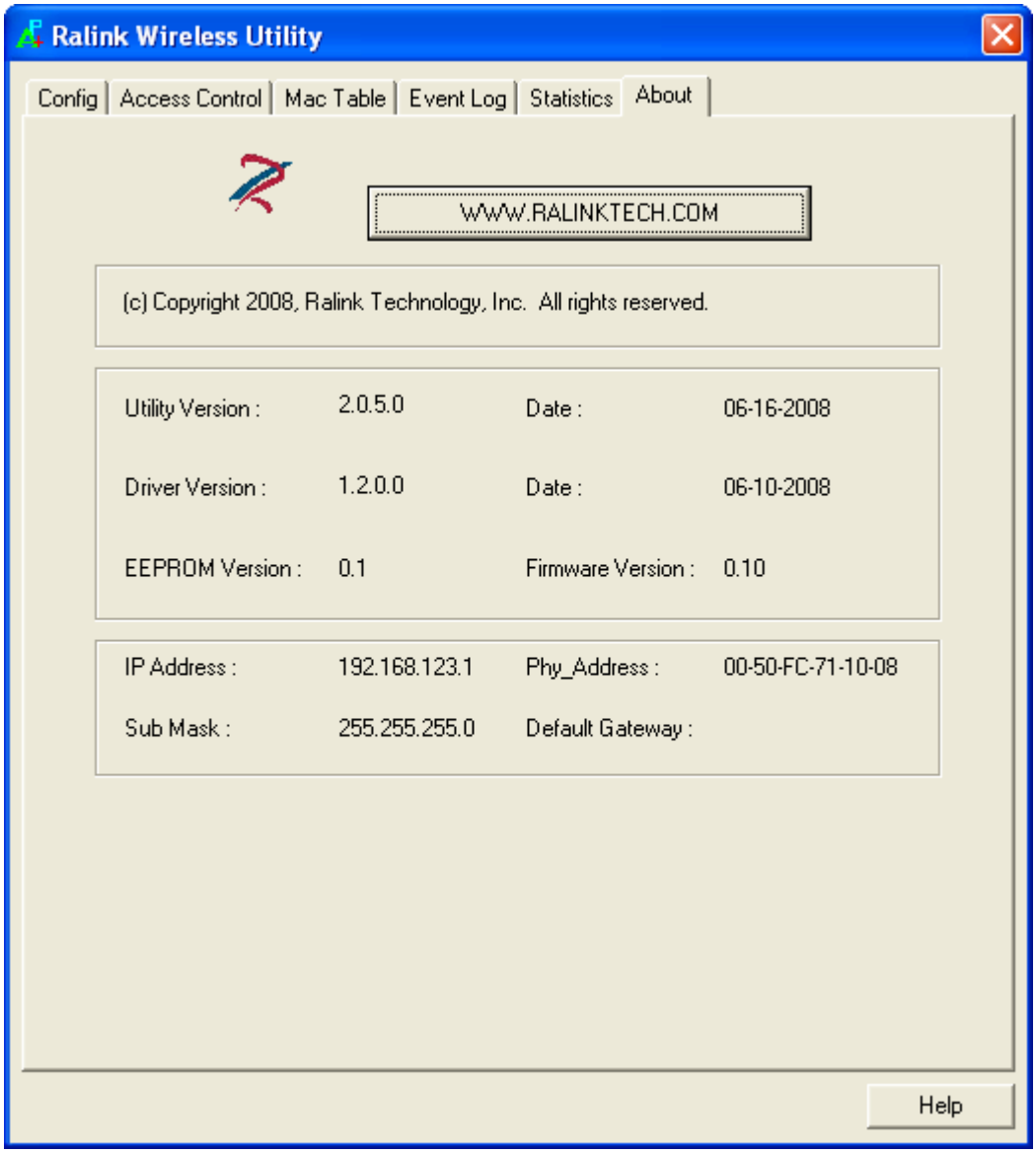
If you want to know detailed information about how your software access point works, click ‘Statistics’ tab, and the event log will be displayed.


Ralink Wireless Utility
Config
Access Control
Mac Table
Event Log
Statistics
About
Transmit Statistics
Frames Transmitted Successfully = 23078
Frames Fail To Receive ACK After All Retries = 127
RTS Frames Successfully Receive CTS = 0
RTS Frames Fail To Receive CTS = 0
Frames Transmitted Successfully After Retry = 1184
Receive Statistics
Frames Received Successfully = 187
Frames Received With CRC Error = 8383
Frames Dropped Due To Out-of-Resource = 0
Duplicate Frames Received = 0
RESET COUNTERS
Help

You can click ‘RESET COUNTERS’ button to reset all counters to zero.

3-7 About

The ‘About’ tab provides you the information about version number of the configuration utility, driver, and other important information about your wireless access point.



CHAPTER IV: Appendix

4-1 Specification

Standards: IEEE 802.11b/g/n (1T1R)
Interface: 32Bit PCI
Frequency Band: 2.4000 ~ 2.4835GHz (Industrial Scientific Medical Band)
Data Rate: 11b: 1/2/5.5/11Mbps
11g: 6/9/12/24/36/48/54Mbps
11n (20MHz): MCS0-7 (up to 72Mbps)
11n (40MHz): MCS0-7 (up to 150Mbps)
Securities: WEP 64/128-bit, WPA, WPA2
Cisco CCX Support
Antenna: One External Dipole Antenna (1T1R)
Drivers: Windows 2000/XP/Vista/7
LEDs: Link, Tx/Rx
Temperature: 32~104°F (0 ~ 40°C)
Humidity: 10-90% (NonCondensing)
Certification: FCC, CE

4-2 Troubleshooting

If you encounter any problem when you're using this wireless network card, don't panic! Before you call your dealer of purchase for help, please check this troubleshooting table, the solution of your problem could be very simple, and you can solve the problem by yourself!

Scenario	Solution
I can't find any wireless access point / wireless device in 'Site Survey' function.	1. Click 'Rescan' for few more times and see if you can find any wireless access point or wireless device. 2. Please move closer to any known wireless access point. 3. 'Ad hoc' function must be enabled for the wireless device you wish to establish a direct wireless link. 4. Please adjust the position of the antenna and click 'Rescan' button for few more times.
Nothing happens when I click 'Launch config utilities'	1. Please make sure the wireless network card is firmly inserted into your computer's PCI slot. If the Ralink configuration utility's icon is black, the network card is not detected by your computer. Switch the computer off and insert the card again. If this doesn't work, contact the dealer of purchase for help. 2. Reboot the computer and try again. 3. Remove the driver and re-install. 4. Contact the dealer of purchase for help.
I can not establish connection with a certain wireless access point	1. Click 'Connect' for few more times. 2. If the SSID of access point you wish to connect is hidden (nothing displayed in 'SSID' field in 'Site Survey' function), you have to input correct SSID of the access point you wish to connect. Please contact the owner of access point to ask

	for correct SSID. 3. You have to input correct passphrase / security key to connect an access point with encryption. Please contact the owner of access point to ask for correct passphrase / security key. 4. The access point you wish to connect only allows network cards with specific MAC address to establish connection. Please go to ‘About’ tab and write the value of ‘Phy_Addess’ down, then present this value to the owner of access point so he / she can add the MAC address of your network card to his / her access point’s list.
The network is slow / having problem when transferring large files	1. Move closer to the place where access point is located. 2. Enable ‘Wireless Protection’ in ‘Advanced’ tab. 3. Disable ‘Tx Burst’ in ‘Advanced’ tab. 4. Enable ‘WMM’ in ‘QoS’ tab if you need to use multimedia / telephony related applications. 5. Disable ‘WMM – Power Save Enable’ in ‘QoS’ tab. 6. There could be too many people using the same radio channel. Ask the owner of the access point to change the channel number. Please try one or more solutions listed above.

4-3 Glossary

1. **What is the IEEE 802.11g standard?**

   802.11g is the new IEEE standard for high-speed wireless LAN communications that provides for up to 54 Mbps data rate in the 2.4 GHz band. 802.11g is quickly becoming the next mainstream wireless LAN technology for the home, office and public networks. 802.11g defines the use of the same OFDM modulation technique specified in IEEE 802.11a for the 5 GHz frequency band and applies it in the same 2.4 GHz frequency band as IEEE 802.11b. The 802.11g standard requires backward compatibility with 802.11b.

   The standard specifically calls for:

   A. A new physical layer for the 802.11 Medium Access Control (MAC) in the 2.4 GHz frequency band, known as the extended rate PHY (ERP). The ERP adds OFDM as a mandatory new coding scheme for 6, 12 and 24 Mbps (mandatory speeds), and 18, 36, 48 and 54 Mbps (optional speeds). The ERP includes the modulation schemes found in 802.11b including CCK for 11 and 5.5 Mbps and Barker code modulation for 2 and 1 Mbps.
   B. A protection mechanism called RTS/CTS that governs how 802.11g devices and 802.11b devices interoperate.

2. **What is the IEEE 802.11b standard?**

   The IEEE 802.11b Wireless LAN standard subcommittee, which formulates the standard for the industry. The objective is to enable wireless LAN hardware from different manufactures to communicate.

3. **What does IEEE 802.11 feature support?**

   The product supports the following IEEE 802.11 functions:

   - CSMA/CA plus Acknowledge Protocol
   - Multi-Channel Roaming
   - Automatic Rate Selection
   - RTS/CTS Feature
   - Fragmentation
   - Power Management

4. **What is Ad-hoc?**

   An Ad-hoc integrated wireless LAN is a group of computers, each has a Wireless LAN card, Connected as an independent wireless LAN. Ad hoc wireless LAN is applicable at a departmental scale for a branch or SOHO operation.

5. What is Infrastructure?

An integrated wireless and wireless and wired LAN is called an Infrastructure configuration. Infrastructure is applicable to enterprise scale for wireless access to central database, or wireless application for mobile workers.

6. What is BSS ID?

A specific Ad hoc LAN is called a Basic Service Set (BSS). Computers in a BSS must be configured with the same BSS ID.

7. What is WEP?

WEP is Wired Equivalent Privacy, a data privacy mechanism based on a 40 bit shared key algorithm, as described in the IEEE 802 .11 standard.

8. What is TKIP?

TKIP is a quick-fix method to quickly overcome the inherent weaknesses in WEP security, especially the reuse of encryption keys. TKIP is involved in the IEEE 802.11i WLAN security standard, and the specification might be officially released by early 2003.

9. What is AES?

AES (Advanced Encryption Standard), a chip-based security, has been developed to ensure the highest degree of security and authenticity for digital information, wherever and however communicated or stored, while making more efficient use of hardware and/or software than previous encryption standards. It is also included in IEEE 802.11i standard. Compare with AES, TKIP is a temporary protocol for replacing WEP security until manufacturers implement AES at the hardware level.

10. Can Wireless products support printer sharing?

Wireless products perform the same function as LAN products. Therefore, Wireless products can work with Netware, Windows 2000, or other LAN operating systems to support printer or file sharing.

11. Would the information be intercepted while transmitting on air?

WLAN features two-fold protection in security. On the hardware side, as with Direct Sequence Spread Spectrum technology, it has the inherent security feature of scrambling. On the software side, WLAN series offer the encryption function (WEP) to enhance security and Access Control. Users can set it up depending upon their needs.

12. What is DSSS? What is FHSS? And what are their differences?

Frequency-hopping spread-spectrum (FHSS) uses a narrowband carrier that changes frequency in a pattern that is known to both transmitter and receiver. Properly synchronized, the net effect is to maintain a single logical channel. To an unintended receiver, FHSS appears to be short-duration impulse noise. Direct-sequence spread-spectrum (DSSS) generates a redundant bit pattern for each bit to be transmitted. This bit pattern is called a chip (or chipping code). The longer the chip is, the greater the probability that the original data can be recovered. Even if one or more bits in the chip are damaged during transmission, statistical techniques embedded in the radio can recover the original data without-the need for retransmission. To an unintended receiver, DSSS appears as low power wideband noise and is rejected (ignored) by most narrowband receivers.

13. What is Spread Spectrum?

Spread Spectrum technology is a wideband radio frequency technique developed by the military for use in reliable, secure, mission-critical communication systems. It is designed to trade off bandwidth efficiency for reliability, integrity, and security. In other words, more bandwidth is consumed than in the case of narrowband transmission, but the trade off produces a signal that is, in effect, louder and thus easier to detect, provided that the receiver knows the parameters of the spread-spectrum signal being broadcast. If a receiver is not tuned to the right frequency, a spread –spectrum signal looks like background noise. There are two main alternatives, Direct Sequence Spread Spectrum (DSSS) and Frequency Hopping Spread Spectrum (FHSS).

14. What is WMM?

Wi-Fi Multimedia (WMM), a group of features for wireless networks that improve the user experience for audio, video and voice applications. WMM is based on a subset of the IEEE 802.11e WLAN QoS draft standard. WMM adds prioritized capabilities to Wi-Fi networks and optimizes their performance when multiple concurring applications, each with different latency and throughput requirements, compete for network resources. By using WMM, end-user satisfaction is maintained in a wider variety of environments and traffic conditions. WMM makes it possible for home network users and enterprise network managers to decide which data streams are most important and assign them a higher traffic priority.

15. What is WMM Power Save?

WMM Power Save is a set of features for Wi-Fi networks that increase the efficiency and flexibility of data transmission in order to conserve power. WMM Power Save has been optimized for mobile devices running latency-sensitive applications such as voice, audio, or video, but can benefit any Wi-Fi device. WMM Power Save uses mechanisms included in the IEEE 802.11e standard and is an enhancement of IEEE 802.11 legacy power save. With WMM Power Save, the same amount of data can be transmitted in a shorter time while allowing the Wi-Fi device to remain longer in a low-power "dozing" state.

16. What is GI?

GI stands for Guard Interval. It's a measure to protect wireless devices from cross- interference. If there are two wireless devices using the same or near channel, and they are close enough, radio interference will occur and reduce the radio resource usability.

17. What is STBC?

STBC stands for Space-Time Block Coding, which is a technique used to transfer multiple copies of data by multiple antenna, to improve data transfer performance. By using multiple antennas, not only data transfer rate is improved, but also the wireless stability.

18. What is WPS?

WPS stands for Wi-Fi Protected Setup. It provides a simple way to establish unencrypted or encrypted connections between wireless clients and access point automatically. User can press a software or hardware button to activate WPS function, and WPS-compatible wireless clients and access point will establish connection by themselves. There are two types of WPS: PBC (Push-Button Configuration) and PIN code.

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

1. Reorient or relocate the receiving antenna.

2. Increase the separation between the equipment and receiver.

3. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

4. Consult the dealer or an experienced radio technician for help.

FCC Caution

This device and its antenna must not be co-located or operating in conjunction with any other antenna or transmitter. This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation. Any changes or modifications not expressly approved by the party responsible for compliance could void the authority to operate equipment.

Federal Communication Commission (FCC) Radiation Exposure Statement

This equipment complies with FCC radiation exposure set forth for an uncontrolled environment. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not

be less than 20cm (8 inches) during normal operation.

The antenna(s) used for this transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

R&TTE Compliance Statement

This equipment complies with all the requirements of DIRECTIVE 1999/5/EC OF THE EUROPEAN PARLIAMENT AND THE COUNCIL of March 9, 1999 on radio equipment and telecommunication terminal Equipment and the mutual recognition of their conformity (R&TTE)
The R&TTE Directive repeals and replaces in the directive 98/13/EEC (Telecommunications Terminal Equipment and Satellite Earth Station Equipment) As of April 8, 2000.

Safety

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this and of the computer manufacture must therefore be allowed at all times to ensure the safe use of the equipment.

EU Countries Intended for Use

The ETSI version of this device is intended for home and office use in Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Luxembourg, Bulgaria, Cyprus, Czech Republic, Estonia, Hungary, Latvia, Lithuania, Malta, Poland, Romania, Slovakia, Slovenia, the Netherlands, Portugal, Spain, Sweden, and the United Kingdom.

The ETSI version of this device is also authorized for use in EFTA member states: Iceland, Liechtenstein, Norway, and Switzerland.

EU Countries not intended for use

None

Please check the declaration of conformity on www.getnet.com.tw

getnet
www.getnet.com.tw

EDIMAX Technology Co., Ltd.

www.getnet.com.tw